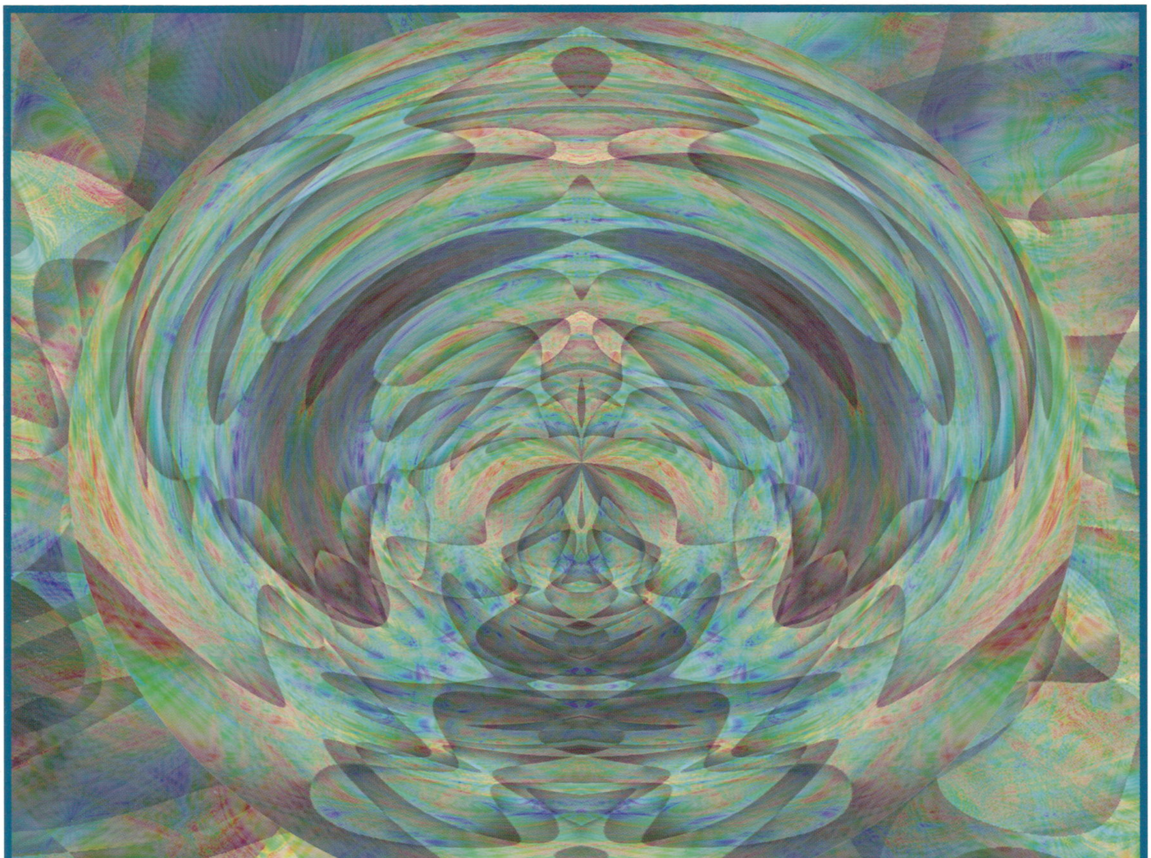
昭和38年7月2日第3種郵便物認可
2014年5月1日発行　第52巻5号　毎月1回1日発行
ISSN 0386—2240

数理科学

5
2014

特集
数理科学における代数的構造
多彩な代数学的アプローチを探る



No.611

サイエンス社

臨時別冊・数理科学（SGC ライブラリ-105：for Senior & Graduate Courses）

ディラック方程式

相対論的量子力学と量子場理論

日笠　健一　著

定価 2479 円

前半は波動方程式としてのディラック方程式について述べ，後半は場の理論におけるディラック場を，ヴァイル場，マヨラナ場とともに解説．素粒子理論で重要な役割を果たすスピン 1/2 の粒子を理論的にどのように記述するかについて基礎的な部分をまとめた．論理的に飛躍がなく，かつすっきりした記述と，細かい計算の丁寧な展開を心がけて書かれた好著．

サイエンス社

MATHEMATICAL SCIENCES
Number 611 May 2014

数理科学における代数的構造

多彩な代数学的アプローチを探る

表紙：戸川　隼人

お得な定期購読をおすすめします

毎号確実に御手元へ

地域によって書店店頭に陳列されない場合があります．**郵送料小社負担**にて確実に御手元へ届く定期予約購読をおすすめします．

予約購読は１年間（本誌のみ）11,000 円，半年間（本誌のみ）5,500 円．（税込み価格）

造本コストは更に上昇気味です．小社としてもあらゆる努力をもって廉価で提供してゆきたいと思っておりますが，定価改定の止むなき事態がかんがえられます．この場合予約購読期間中のものにつきましては料金据置きとなります．なお，臨時別冊のご注文については，本誌予約購読者の方には，商品到着後のお支払いにて承ります．

お申し込みは本誌とじ込みの振替用紙を御利用下さい．

数理科学特集一覧

63 年/7〜2011 年/6 省略
2011 年/7 〈隠れた〉物理法則
/8 計算が拓く数学と物理の世界
/9 オイラー
/10 時空と熱力学
/11 線形から非線形へ
/12 物理と仮説
2012 年/1 数学から物理へ，物理から数学へ
/2 古典のススメ［物理編］
/3 量子を操る
/4 量子力学の数学的技法
/5 解析学と物理学
/6 面白い発想［物理編］
/7 数学と物理における格子
/8 導来圏をめぐって
/9 ハイゼンベルク
/10 超弦理論の数理
/11 物理と数学における厳密解
/12〈振動する〉物理
2013 年/1 表現論の世界
/2 《量子化》の発想
/3 光と物理学
/4 解析学における様々な発想
/5 次元の作法
/6 発展する統計力学
/7 群と物理学
/8 エネルギーを通して物理学を知る
/9 ボーア
/10 分類する《数理科学》
/11 理論物理と実験物理の交錯
/12 物理学における存在とは
2014 年/1 波と粒子
/2 利用する物理
/3 幾何学における様々な発想
/4 物理現象における表現の多様さ

数理科学臨時別冊一覧

12 年/12 量子力学から超対称性へ
13 年/1 行列解析ノート
13 年/4 無限量子系の物理と数理
13 年/7 現代宇宙論講義
13 年/8 クォーク・ハドロン物理学入門
13 年/9 統計力学から理解する　超伝導理論
13 年/12 量子力学ノート
14 年/1 量子情報と時空の物理
14 年/2 弦理論と行列模型
14 年/3 ディラック方程式
14 年/4 ホログラフィー原理と量子エンタングルメント

「数理科学」のバックナンバーは下記の書店・生協の自然科学書売場で特別販売しております

紀伊國屋書店本店（新宿）
紀伊國屋書店新宿南店
あおい書店中野本店
オリオン書房ノルテ店（立川）
くまざわ書店八王子店
くまざわ書店桜ヶ丘店（多摩）
書泉グランデ（神田）
三省堂本店（神田）
リブロ池袋店
ジュンク堂池袋本店
芳林堂（高田馬場）
MARUZEN ＆ジュンク堂渋谷店
八重洲ブックセンター（東京駅前）
丸善丸の内本店（東京駅前）
丸善日本橋店
MARUZEN 多摩センター店
ジュンク堂吉祥寺店
ブックファースト青葉台店（横浜）
有隣堂イセザキ町本店（横浜）
有隣堂西口・東口（横浜）
有隣堂厚木店（厚木）
ジュンク堂盛岡店
丸善津田沼店
ジュンク堂新潟店
ジュンク堂甲府岡島店
MARUZEN ＆ジュンク堂新静岡店
戸田書店静岡本店
ジュンク堂大阪本店
紀伊國屋書店梅田店（大阪）
アバンティブックセンター（京都）
ジュンク堂京都店
ジュンク堂三宮店
ジュンク堂三宮駅前店
ジュンク堂大分店
喜久屋書店倉敷店
MARUZEN 広島店
紀伊國屋書店福岡本店
ジュンク堂福岡店
丸善博多店
ジュンク堂鹿児島店
紀伊國屋書店新潟店
ジュンク堂旭川店
金港堂（仙台）
金港堂パーク店（仙台）
ジュンク堂仙台本店
ジュンク堂秋田店
ジュンク堂郡山店
鹿島ブックセンター（いわき）
友朋堂（つくば）

——大学生協・売店——
東京大学 本郷・駒場
東京工業大学 大岡山・長津田
東京理科大学 新宿
早稲田大学 理工学部
慶応義塾大学 矢上台
福井大学
筑波大学 大学会館書籍部 第一学群書籍部
埼玉大学
名古屋工業大学・愛知教育大学
大阪大学・神戸大学 ランス
京都大学・九州工業大学
東北大学 理薬・工学
室蘭工業大学
徳島大学 常三島
愛媛大学 城北
山形大学 小白川
島根大学
学習院大学 成文堂
北海道大学 クラーク店
熊本大学
名古屋大学
広島大学（北１店）
九州大学（理系）

MATHEMATICAL SCIENCES
May 2014 Number 611

特集／数理科学における代数的構造

代数学からのアプローチ

桂　利行

20世紀のフランスにおいて，構造主義を掲げて数学の基礎の再編を図った数学者集団がある．ブルバキである．アンリ・カルタン，クロード・シュヴァレー，ジャン・デルサルト，ジャン・デュドネ，アンドレ・ヴェイユという錚々たるメンバーによって始められたこの活動は，ジャン・ピエール・セール，ピエール・カルチエなどの世界トップレベルの数学者と世代交代を重ねつつ，20世紀の数学に大きな影響を与えた．彼らは，代数構造，順序構造，位相構造という3つの大きな型を設定し，それに基づいて約7000ページにもおよぶ「数学原論」を著し数学の体系化を図った[1]．その根幹には，数学を純化すれば代数になるという考え方があるように思われる．実際，どのような数学にもどこかに代数的な構造が存在すると言っても過言ではなく，また，代数的構造は数学の理論を体系化するのに大変都合がよい．A.F.モンナもその著書『現代数学発展史』[2]において，古典数学から現代数学への発展の過程で数学の代数化が果たした役割の重要性について述べている．現在では，ブルバキ的な考え方に対する批判も多く，解析や幾何においては代数では扱いきれない部分が多々あることも事実であるが，代数化できる部分には構造的な数学美が秘められている．

それでは，自然界や社会に存在する数理科学には，どのくらい代数的な構造があるだろうか．代数とは基本的には演算の数学であり，整数や多項式と関係した概念がその根底に存在する．このように基本的なものであるがゆえに，数学的に把握できるところには何らかの意味で代数構造が存在するし，対称性が存在するところには面白い代数構造が潜んでいる．また，アルゴリズムという用語は，algebra（代数）という言葉の語源となったアラビア語 Al-jabr（移項）という用語を著書に用いたアル・フワーリズミーの名前から生まれたが，代数はアルゴリズムを作るのに都合がよい分野でもある．アルゴリズムを見出すことは，ルーティーン化をすることに他ならない．これは，人間の思考を簡略化するだけではなく，コンピュータとも相性が良い．代数化は異なる分野間の類似を見出すという効果もある．本特集号では，数理科学における代数構造に着目し，素粒子物理学，情報科学における暗号理論・学習理論・コンピュータ理論，生命科学や結晶構造の化学など，現在展開されている研究から代数構造が効果的に使われているものを選んでご紹介する．

素粒子論においては，古典的な運動方程式の範囲ではもはや理論は組み立てられず，量子力学が必要になる．ヒルベルト空間とその上の自己共役作用素という量子力学の設定は代数が有効に働く環境である．物理系の状態にはヒルベルト空間の状態ベクトルが，物理量には自己共役作用素が対

応し，自己共役作用素の固有値が観測値となる．また，リー群やリー環の表現論が重要な役割を演じ（菅野浩明氏の論説参照)，素粒子を点ではなく弦として捉える超弦理論（スーパーストリング理論）では，代数曲線（リーマン面）やカラビ・ヤウ多様体などの代数幾何学の対象が躍動している．

かつては，暗号というと国家間の闘争に用いられる暗いイメージであった．ここで用いられていたのは，暗号化と解読の鍵を通信の当事者間で共有する共通鍵暗号であった．1976 年にディフィーとヘルマンは，不特定多数の人の中で暗号化の鍵を公開しても，その鍵を使って任意の 2 人が秘密裏に暗号通信を行うことが可能であるという理論を発表した．これが，公開鍵暗号であり，インターネットが発達した現在にあっては，その代表格である RSA 暗号などが通信のために欠かせない道具となっている．ここでは，初等整数論を初めとする代数学が有効に用いられている（内山成憲氏の論説参照)．数論は，かつては数学の女王として君臨していたが，現在ではこのような実用の世界で役割を果たしていることは興味深い．また，力学系の世界にも数論の視点が持ち込まれ，様々な現象が解析されている（川口周氏の論説参照)．

情報の世界にも様々な代数構造が存在する．現代社会では，コンピュータは欠くことのできない道具であるが，その学習理論（小林正典氏の論説参照）や計算機システムの正しさを数学的に証明することを目標とした形式検証の理論では代数学が重要な役割を果たしている（蓮尾一郎氏の論説参照)．生命科学では，粗視化という離散化のテクニックが用いられている．こうすることによって複雑な現象が整理され，対象に代数的な構造を見出すことが可能になる（加藤毅氏の論説参照)．化学の世界でも結晶構造の対称性を解析するために代数学の理論が有効に働いており，新しい結晶体の探索が行われている（小田忠雄氏の論説参照)．本特集号では，ご紹介できなかったが，デジタル機器の正常な作動を保証する誤り訂正符号理論では，有限体上のベクトル空間とその部分空間の理論が本質的に用いられているし，可積分系におけるソリトン（孤立波）の理論にも美しい代数構造が見出されている．

代数と幾何は古くから人類に用いられてきた．現在においても，それらは初等教育における中心的な学習の題材であり，代数は，ほとんどすべての数学で用いられる強力な道具である．代数の魔力とその危険性について，1966 年にフィールズ賞を受賞した幾何学者アティヤは，ゲーテのファウストに準えて次のように言っている：「代数は，悪魔が数学者に手渡した贈り物である．」[3] ファウスト博士は魂と引き換えに若さを得た．悪魔は幾何学者に言う．私はあなたにこの強力な道具をあげよう．このマシーンはすべての質問に答えてくれるだろう．それを使うために，あなたがすべきことは魂をくれることだ．すなわち，幾何をやめればこのマシーンを渡そう．——この言葉は，代数に安易に走ることへの警鐘でもある．幾何に代数を持ち込んで考察すると，代数の計算に没頭することによって証明が完結することもあるが，そこには幾何学的な本質を見失う危険性が潜んでいる．しかし，それでも代数構造を様々な領域で見出し，それを有効に用いることによって様々な問題を解決することは，数理科学の発展にとって必要不可欠なことであろう．

参考文献

1) M. マシャル著，高橋礼司訳『ブルバキ　数学者達の秘密結社』，シュプリンガー・ジャパン，2002 年．
2) A.F. モンナ著，鶴見和之・新井理生共訳『現代数学発展史　現代数学の進展―方法・概念・思想の変遷』，東京電機大学出版局，1993 年．
3) マイケル・F. アティヤ著，志賀浩二編訳『数学とは何か』，朝倉書店，2010 年．

（かつら・としゆき，法政大学理工学部）

素粒子のスピンと表現論
ディラック方程式とクリフォード代数



菅野 浩明

1. はじめに

最近の素粒子論における最大の話題といえば，何といってもCERNの大型加速器LHCにおけるヒッグス粒子[*1]の発見（実験的検証）でしょう．昨年のノーベル物理学賞がF. Englert, P.W. Higgsの両博士にいち早く授与されたことは，そのインパクトの大きさを強く印象付けるものです．ヒッグス粒子はいわゆる素粒子の標準模型において存在が予言されながら，未発見であった最後の素粒子であり，その発見は素粒子の標準模型の最後のピースを埋めたとも言われます．ところでヒッグス粒子は素粒子の標準模型において，非常にユニークな性質を持っています．すなわち，そのスピンが0であることです．ヒッグス粒子はゼロでない（非自明な）真空期待値をもつことにより，素粒子に質量を与えるとされていますが，真空期待値を持つことが可能であるのは，ヒッグス粒子のスピンが0であるためであり，0でないスピンをもつ他の素粒子には真似のできないことです．

素粒子の標準模型において，ヒッグス粒子以外の素粒子は物質を構成する粒子と粒子間に働く力を媒介する粒子のいずれかに分類されます．前者はすべてスピン1/2をもちフェルミ粒子と呼ばれます．一方，後者はすべてスピン1をもちゲージ粒子（ゲージボソン）と呼ばれます．素粒子の標準模型を越える物理の候補として超対称性が有名です．実際，ヒッグス粒子の探索とともに超対称粒子の探索がLHCの当初の目標でした．超対称性はスピン1/2をもつフェルミ粒子とスピン1をもつゲージボソンを対等なものとして扱い，標語的に物質と力の統一が実現されるとも言われますが，この観点からするとスピンが0であるヒッグス粒子は“仲間はずれ”ということになります．ヒッグス粒子の正体が何であるか，とりわけ本当に基本粒子であるかは，今後LHCにおける実験データの蓄積とともに，大きな問題となると思いますが，ここでは素粒子論と代数学の関わりとして量子論と表現論との関係を取り上げ，とくに特殊相対性理論におけるローレンツ対称性の表現という観点から，上に登場した素粒子のスピンについて説明します．具体的には，スピン1/2をもつフェルミ粒子に対する量子力学的基礎方程式であるディラック方程式とスピン表現を定義する上で必要となるクリフォード代数について紹介したいと思います．本稿では詳しく述べる余裕がありませんが，一般次元のクリフォード代数は超対称性や超弦理論の代数的構造を記述する際に重要な役割を果たします．

2. 量子論と表現論

素粒子論に限らず，現代物理学において最も重要な考え方は対称性です．数理物理学における大

*1） 正確にはHiggs-like particleと発表されています．

きな分野として可積分系の理論がありますが，ここでは対称性のみを頼りに系のエネルギー固有値や相関関数といった物理量を決定することが問題とされます．対称性は数学的には群の概念を用いて考えることができます．以下では群 G の元が連続的なパラメータをもち，それについて微分が意味をもつ場合を考えることにします．このような群を**リー群**と呼び，2 次元や 3 次元空間の回転全体からなる群が典型的な例です．量子論においてはリー群 G（あるいはその無限小生成子全体のなすリー代数）の表現を考える必要があります．以下でその理由を見てみましょう．

古典論では粒子の状態はある時刻 t における位置 $x(t)$ や運動量 $p(t)$ で与えられると考え，その運動は $x(t)$ や $p(t)$ の時間変化を追うことによって記述されると考えます．このため古典論の運動方程式は，時間 t の関数である $x(t)$ や $p(t)$ に対する微分方程式となっています．これに対して量子論ではある時刻において確定するのは我々が実際に観測する物理量ではなく**状態ベクトル**と呼ばれる抽象的な量 $\Phi(t)$ であると考えます*2)[1]．次節で述べるように，量子論の基礎方程式であるシュレディンガー方程式は状態ベクトル $\Phi(t)$ の時間変化を与える方程式となっています．状態“ベクトル”という名前は $\Phi(t)$ が内積をもつ複素ベクトル空間（ヒルベルト空間）の元であることに由来します．ベクトルのもつ重要な特性は，それらの重ね合わせ（線形結合）が意味を持つことですが，状態の重ね合わせを考えることができるという点は量子論に特有の現象を説明するために重要になります．

さて，量子論において考えたい対称性に対応する群 G の元 g を考え，g によって量子論の状態ベクトル Φ が $\rho(g)\Phi$ に移ったとします．例えば空間の回転により状態ベクトル Φ がどう変化するかを考えると思えばよいでしょう．すなわち $\rho(g)$ で g がヒルベルト空間上に引き起こす写像を表すことにします．ここですべての $g \in G$ に対して

*2)　正確には $\Phi(t)$ とその複素定数倍を同一視する同値類が状態に対応すると考えます．

$\rho(g)$ が線型写像となるとき，対称性は**線型実現**されているといいます．量子論において，対称性は必ずしも線型実現されているとは限りません．例えば「対称性の自発的破れ」という言葉を聞いたことがある読者の方も多いと思いますが，この場合，対称性は一般に非線型に実現されています．以下では簡単のため対称性は線型に実現されている場合のみを考えます．

量子論で現れるヒルベルト空間 $\mathcal{H}$ は一般に無限次元ですが，ある対称性だけに着目すると，多くの場合，有限次元ベクトル空間 $\mathcal{V}_n$ の族を用いて

$$\mathcal{H} = \bigoplus_{n\in\mathbb{Z}} \mathcal{V}_n \tag{1}$$

と直和分解されたり，有限次元ベクトル空間 $\mathcal{U}$ が存在して

$$\mathcal{H} = \mathcal{H}' \otimes \mathcal{U} \tag{2}$$

とテンソル積に分解されます．前者では添え字 n は対称性によって保存される“量子数”を象徴的に表しています．例えば，量子力学の教科書にある水素原子の固有状態を求める問題では，対称性は 3 次元空間の回転群 $SO(3)$ であり $n > 0$ は主量子数と呼ばれています．また $\mathcal{V}_n$ は $2n^2$ 次元で，エネルギー固有値は n のみに依存しています[2]．一方，後者の例は以下で紹介するディラック方程式における状態ベクトルの扱いに見ることができます．このとき対称性は $\mathcal{H}'$ に自明に働き，$\mathcal{U}$ は 4 次元ベクトル空間です．以下ではベクトル空間としては有限次元のものを考えます．このとき基底をとることにより $\rho(g)$ は行列を用いて表すことができるようになるので扱いが簡単になります．

さて群の 2 つの元 g, h に対して，その積 gh を表す行列 $\rho(gh)$ は各々の元に対応する線型写像の合成で与えられると考えられます．一方，線型写像の合成が行列の積 $\rho(g)\rho(h)$ で表されるので

$$\rho(g)\rho(h) = \rho(gh) \tag{3}$$

が成り立つはずです．すなわち量子論において対称性が線型実現されているとき，これは次の意味で状態ベクトル全体のなすヒルベルト空間 V 上

の群 G の表現を与えます[3,4].

> **定義**：群 G と複素ベクトル空間 V に対して写像 $\rho : G \to GL(V)$ が群の準同型となるとき，すなわち $\rho(a)\rho(b) = \rho(ab)$ が成り立つとき (V, ρ) を G の（複素）表現という．ここで $GL(V)$ は V 上の正則な線型変換全体のなす群である．

量子論では複素ベクトル空間 V に内積が定義されていて，観測値は状態ベクトルからこの内積を用いて計算されます．したがって群 G が量子論的対称性であるということを G の作用 $\rho(a)$ によって観測値が不変であることとするならば，$\rho(a)$ は内積を保つ線型変換，すなわちユニタリ行列であることになります．このとき特に (V, ρ) を G の**ユニタリ表現**といいます．ところで我々が実際に観測できるのは，状態ベクトルの無限小変化である場合がほとんどです．その意味で，物理的により重要な意味をもつのはユニタリ行列 $\rho(a)$ の微分に当たる量になります．数学的にはこれは（リー）群の無限小生成子全体のなすリー代数と呼ばれます．無限小生成子を表す行列 L はリー群の元 a をパラメータ t を用いて $a(t)$ とするとき

$$\rho(a(t)) = \exp(\sqrt{-1}tL) \tag{4}$$

の関係式を満たします．ここで正方行列 A の指数関数を

$$\exp A := \sum_{n=0}^{\infty} \frac{A^n}{n!} \tag{5}$$

で定義しました．$\exp A$ は A と同じサイズの正方行列です．この定義を用いると $\rho(a(t))$ がユニタリ行列であることと L がエルミート行列となることは同値であることが分かります．量子力学では物理量はエルミート演算子で与えられると考えますので，この L が物理量に対応することになります．

3. 量子論の確率解釈とディラック方程式

前節で述べたように，量子論では系の状態は状態ベクトルと呼ばれるヒルベルト空間の元 Φ により表されます．その時間発展を記述するのが有名な**シュレジンガー方程式**

$$\sqrt{-1}\frac{\partial}{\partial t}\Phi = H\Phi \tag{6}$$

です．ここで H はヒルベルト空間上の線型作用素で，正準変数（一般化座標と共役運動量）を用いて古典力学のハミルトニアンが与えられていれば，共役運動量を対応する座標に関する微分（の $-\sqrt{-1}$ 倍）とする対応原理により定まります．例えばポテンシャル $V(x)$ をもつ保存力の下での質量 m の粒子のハミルトニアンは

$$H = -\frac{1}{2m}\nabla^2 + V(x), \quad x \in \mathbb{R}^3 \tag{7}$$

です．前節では量子論では状態の重ね合わせを考えることができるという点が重要であることを強調しましたが，H が線型であることは時間発展に関して状態の重ね合わせが保存されることを意味しています．また H が時間 t に依存しないとき，方程式 (6) の解は形式的に

$$\Phi(t) = \exp(-\sqrt{-1}\,tH)\Phi(0) \tag{8}$$

と書けますが，この式と無限小生成子 L に対する関係式 (4) の類似性にも注意してください．

ここで注意しておきたいのは，方程式 (6) において H は必ずしも古典力学のハミルトニアンから，対応原理により得られるものと限る必要はないことです．すなわち方程式 (6) は状態ベクトル Φ に対する抽象的な時間発展方程式とみなすことができるという点です．このとき H に対して要求される性質はエルミート $H^\dagger = H$ であることです．これは次のような量子論の確率解釈と関係しています．量子論における確率密度 ρ は状態ベクトルにより

$$\rho(x,t) = |\Phi(x,t)|^2 = \Phi(x,t)^*\Phi(x,t) \tag{9}$$

で与えられます．これは系が状態ベクトル Φ で表される状態にあるとき，空間のある領域 V に粒子を見出す確率が

$$\int_V d^3x\ \rho(x,t) \tag{10}$$

で与えられるということです．特に空間全体に渡って積分すれば全体の確率は 1 で，これは時間によらず一定でなければなりません．すなわち

$$\frac{d}{dt}\int_{\mathbb{R}^3} d^3x\ \rho(x,t) = 0 \tag{11}$$

が成り立たなければなりませんが，(6) とハミルトニアンのエルミート性を用いて

$$\frac{d}{dt}\int_{\mathbb{R}^3} d^3x\ \rho = \int_{\mathbb{R}^3} d^3x \left(\frac{\partial \Phi^*}{\partial t}\Phi + \Phi^*\frac{\partial \Phi}{\partial t}\right)$$
$$= \int_{\mathbb{R}^3} d^3x \left(\sqrt{-1}H^\dagger\Phi^\dagger\Phi - \sqrt{-1}\Phi^\dagger H\Phi\right) = 0$$

が確かめられます．ハミルトニアンが (7) のように具体的に与えられていると，さらに詳しく**確率密度の保存則**を局所的に見ることができます．すなわち

$$\boldsymbol{j} := \frac{\sqrt{-1}}{2m}\left((\mathrm{grad}\ \Phi^*)\Phi - \Phi^*(\mathrm{grad}\ \Phi)\right) \tag{12}$$

と確率の流れを表す 3 次元ベクトルを定義するとシュレジンガー方程式 (6) から

$$\frac{\partial}{\partial t}\rho + \mathrm{div}\ \boldsymbol{j} = 0 \tag{13}$$

を確かめることができます．興味深いことは，局所的な確率密度の保存則 (13) が次のような意味で，すでに相対論的な式になっていることです．すなわち ρ を 4 元カレントの時間成分と見なして $j^\mu = (\rho, \boldsymbol{j})$ とすれば，ミンコフスキー空間の座標 $x^\mu = (t, \boldsymbol{x})$ を用いて (13) を

$$\frac{\partial j^\mu}{\partial x^\mu} = 0 \tag{14}$$

と書くことができます．

一方，シュレジンガー方程式 (6) 自身は相対論的ではないので，これを状態ベクトルに対する時間発展方程式と見なして相対論的な方程式とすることを考えます[5)]．ここでのポイントは上で説明した状態ベクトルに対する確率解釈と両立するように相対論的な書き換えを行うという点です[*3)]．

相対論ではエネルギー E と（3 次元）運動量 $\boldsymbol{p}$ を合わせて 4 元ベクトル $p^\mu = (E, \boldsymbol{p})$ と考えます．ここで粒子の質量を m とするとき

$$p^\mu p_\mu := E^2 - \boldsymbol{p}^2 = \boldsymbol{m}^2 \tag{15}$$

が成り立ちます．したがって状態ベクトルが満たすべき方程式としてまず候補となるのが相対論的に不変なクライン・ゴルドン方程式

$$\frac{\partial^2}{\partial t^2}\Phi + \nabla^2\Phi = 0 \tag{16}$$

です．この方程式の問題点は時間に関して 2 階の微分方程式であることです．このために時間に関して 1 階の微分方程式である (6) に対して行った確率密度の保存に関する議論が成立しなくなってしまいます．実際 (12) の定義と ρ を 4 元カレントの時間成分と見なすという観点から自然な ρ の定義は

$$\rho(t,x) := -\frac{\sqrt{-1}}{2m}\left(\frac{\partial \Phi^*}{\partial t}\Phi - \Phi^*\frac{\partial \Phi}{\partial t}\right) \tag{17}$$

です．実際，クライン・ゴルドン方程式を用いると局所的な確率密度の保存則 (13) を示すことができますが，この ρ は正定値ではないのでもはや確率密度と解釈することができません[*4)]．以下で示されるように，相対論的な書き換えを考える際に確率密度を表す 4 元カレントの定義で保持すべきは ρ のほうであって，変更を受けるべきなのは微分を含む空間成分 $\boldsymbol{j}$ のほうなのです．

量子論的な確率解釈を成り立たせるために，時間に関して 1 階の微分方程式である (6) を保つようにしてみます．また相対論的関係式 (15) を考慮して線型作用素 H を運動量と質量の 1 次式であると仮定します．すなわち

$$H = \alpha_x p_x + \alpha_y p_y + \alpha_z p_z + \beta m \tag{18}$$

とします．これが相対論的関係式 (15) と矛盾なく成り立つためには係数 $\alpha_{x,y,z}$ と β が関係式

*3) 場の量子論を知っている読者向けのコメントです．場の量子論ではここで考えている状態ベクトルを（第 2）量子化するので，場の量子論で確率を表す "状態ベクトル" は本稿で考えているものとは異なります．また場の量子論では粒子の生成や消滅を考えることになるので確率の保存の意味もここで考えているものとは異なることになります．

*4) 場の量子論では，ここで考えた 4 元カレントは電荷密度と電流のペア（$U(1)$ ゲージ対称性に伴う保存カレント）と解釈されます．

$$\alpha_x^2 = \alpha_y^2 = \alpha_z^2 = \beta^2 = 1,$$
$$\alpha_i\alpha_j + \alpha_j\alpha_i = 0 \quad (i \neq j), \qquad (19)$$
$$\alpha_i\beta + \beta\alpha_i = 0$$

を満たさなければなりません．通常の数（スカラー）でこの関係式を満たすことはできませんが，係数が行列であると仮定すれば，このような関係式を満たすものが存在します．そのうち最も簡単なものは4次正方行列で書くことができます．したがって相対論的な時間発展のためには状態ベクトルは4つの成分 $\Psi = (\psi_r)_{r=1,\cdots,4}$ を持つことになり各成分の時間発展は

$$\sqrt{-1}\frac{\partial\psi_r}{\partial t} = \sum_{s=1}^{4}\Big[p_x\alpha_x + p_y\alpha_y + p_z\alpha_z + m\beta\Big]_{rs}\psi_s \qquad (20)$$

となります．これが**ディラック方程式**です．ディラック方程式に従う状態ベクトルは4成分になるので，その確率密度は

$$\rho = \sum_{r=1}^{4}\psi_r^\dagger\psi_r \qquad (21)$$

とするのが自然です．ここで3次元カレントを

$$j_{x,y,z} = \sum_{r=1}^{4}\psi_r^\dagger\alpha_{x,y,z}\psi_r \qquad (22)$$

とすれば，ディラック方程式を用いて確率密度の保存則 (13) を示すことができます．

4. クリフォード代数とローレンツ群のスピン表現

前節では状態ベクトルに対する確率解釈を相対論と矛盾なく成立させるという要請から状態ベクトルに対する時間発展方程式がどうあるべきかを考えてディラック方程式を導きました．そこで必要となったのは関係式 (19) を満たす行列の組 (α_i, β) です．以下ではディラック方程式に従う状態ベクトルが相対性理論の基本的対称性であるローレンツ変換群の下でどのように変換すべきかを調べま

す．その過程で明らかになるのが，ローレンツ群の表現としてのスピン表現と関係式 (19) を満たす行列の組 (α_i, β) の役割です．

クライン・ゴルドン方程式 (16) の場合は関数 Φ にかかる 2 階微分作用素（ダランベール作用素）がローレンツ変換*5)

$$x'_\mu = a_\mu^\nu x_\nu \tag{23}$$

の下で不変なので関数 Φ 自身が変化する必要はありません．本稿の初めにヒッグス粒子のスピンは 0 であるという話を紹介しましたが，相互作用を無視する場合ヒッグス粒子の従う運動方程式はクライン・ゴルドン方程式です．ヒッグス粒子のスピンが 0 であるということはローレンツ変換の下で不変であることを意味しています．一方，スピン 1/2 の素粒子に対する運動方程式であるディラック方程式に現れるのは 1 階の微分作用素で，これはローレンツ変換 (23) の下で共変ベクトルとして変換します．このため 4 成分からなる状態ベクトル Ψ もまた非自明に変換する必要があります．この様子を具体的に見るために，ディラック方程式をローレンツ変換の下での変換性が見やすくなるように書き換えます．**ガンマ行列**を

$$\gamma_j := -\sqrt{-1}\beta\alpha_j \quad (j=1,2,3),\ \gamma_4 := \beta \tag{24}$$

と定義すれば，これらの交換関係は

$$\gamma_\mu\gamma_\nu + \gamma_\nu\gamma_\mu = 2\delta_{\mu\nu}\cdot\mathbf{1} \tag{25}$$

となります．ここで $\mathbf{1}$ は単位行列を表します．このような関係式 (25) で定義される代数は，一般に**クリフォード代数**と呼ばれています*6)．ところで定義式 (25) で $\delta_{\mu\nu} \to 0$ とすれば，この代数は多様体上の微分形式全体のなす代数を典型的な例とする外積代数に一致します．その意味でクリフォード代数を外積代数の“量子化”と見なすことがあります．例えばパラメータの連続的な変化 $\delta_{\mu\nu} \to 0$ で多元環の（ベクトル空間としての）次元は変わらないはずです．したがって上で定義したガンマ行列全体のなすクリフォード代数の次元は 4 次元ベクトル空間に対する外積代数の次元 $1+4+6+4+1=16$ となります．これは 4 次の正方行列全体の次元と一致しています．

話が脇道に逸れてしまいましたが，ガンマ行列を用いてディラック方程式は

$$\left(\gamma_\mu\frac{\partial}{\partial x_\mu} + m\right)\Psi = 0 \tag{26}$$

となります．さてローレンツ変換 (23) の下で 4 成分の状態ベクトルが行列 σ_{rs} を用いて

$$\Psi'_r(x') = \sum_{s=1}^{4}\sigma_{rs}\Psi_s(x) \tag{27}$$

と変換することを仮定します．一方，ローレンツ変換されたディラック方程式は

$$\sum_{s=1}^{4}\left[\sum_{t=1}^{4}(\gamma_\mu)_r^t\sigma_{ts})a_\nu^\mu\frac{\partial\Psi_s}{\partial x_\nu} + m\sigma_{rs}\Psi_s\right] = 0 \tag{28}$$

となるので，これが元の方程式と一致するための条件は

$$\sigma^{-1}\gamma_\mu\sigma = a_\mu^\nu\gamma_\nu \tag{29}$$

となります．この条件 (29) を満たす σ がベクトルにローレンツ変換を表す行列 a_μ^ν に依存することを明示するために $\sigma(a)$ と書くことにします．$\sigma(a)$ がローレンツ群の表現となることは，次のようにして分かります．すなわち，もう一つのローレンツ変換 b_μ^ν に対して条件 (29) と同様の式から定まる行列を $\sigma(b)$ と書けば

$$(\sigma(a)\sigma(b))^{-1}\gamma_\mu\sigma(a)\sigma(b) = a_\mu^\nu b_\nu^\rho\gamma_\rho \tag{30}$$

を確かめることができます．これは

$$\sigma(a)\sigma(b) = \sigma(ab) \tag{31}$$

が成り立つことを意味しており，$\sigma(a)$ はローレン

*5) これ以降，上下の添え字が同じものに対しては 1 から 4 まで和を取るというアインシュタインの規則を使います．

*6) クリフォード代数は一般に内積が定義されたベクトル空間に対して定義されます．(25) 式の右辺の $\delta_{\mu\nu}$ は内積の成分に由来します．

ツ群の 4 次元表現を与えます．これを**スピン表現**と言います．ディラック方程式に従う素粒子がスピン 1/2 を持つことは，状態ベクトルがスピン表現に従って変換することからの帰結です．

先に注意したようにガンマ行列 γ_μ が生成するクリフォード代数の次元は 4 次正方行列全体の次元と一致しているので，スピン表現を表す行列 σ はガンマ行列の多項式で書けているはずです．無限小のローレンツ変換

$$x'_\mu = x_\mu + \epsilon_\mu^\nu x_\nu \tag{32}$$

に対応するスピン表現の行列を無限小パラメータの 1 次までで

$$\sigma(\epsilon) = \mathbf{1} + \epsilon^{\mu\nu} T_{\mu\nu} \tag{33}$$

を仮定します．ここで無限小パラメータ $\epsilon^{\mu\nu}$ は変換がローレンツ変換となることから反対称性 $\epsilon^{\mu\nu} = -\epsilon^{\nu\mu}$ を満たすので $T_{\mu\nu} = -T_{\nu\mu}$ とします．条件式 (29) に無限小形を用いて計算すると

$$T_{\mu\nu} = \frac{1}{4}(\gamma_\mu\gamma_\nu - \gamma_\nu\gamma_\mu) \tag{34}$$

が得られます．一方，ガンマ行列の定義関係式 (25) を用いると交換関係

$$[T_{\mu\nu}, T_{\rho\kappa}] = \delta_{\mu\rho}T_{\nu\kappa} + \delta_{\nu\kappa}T_{\mu\rho} - \delta_{\mu\kappa}T_{\nu\rho} - \delta_{\nu\rho}T_{\mu\kappa} \tag{35}$$

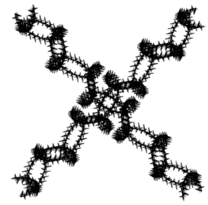
を確かめることができます．ここでは，無限小ローレンツ変換に対応する行列を求めたので，これはローレンツ群のリー代数と関係しているはずですが，実際 (35) は確かにローレンツ群のリー代数が満たす関係式に一致しています．

参考文献

1) 清水明,『新版 量子論の基礎』サイエンス社 (2003).
2) 猪木慶治・川合 光,『量子力学 I』講談社 (1994).
3) 平井武・山下博,『表現論入門セミナー』遊星社 (2003).
4) 林正人,『量子論のための表現論』共立出版 (2014).
5) 西島和彦,『相対論的量子力学』培風館 (1973).

（かんの・ひろあき，名古屋大学大学院多元数理科学研究科）

暗号理論と代数学



内山 成憲

1. はじめに

現在の我々の日々の生活では，インターネットは欠かせないものとなっている．さらに，インターネットを安心かつ安全に利用するためには，暗号技術は不可欠なものである．古来より利用されてきた暗号は，暗号化と復号の際に使用する鍵が同一のものであり，**共通鍵暗号**と呼ばれる．一方，暗号化と復号で使用する鍵が異なり，暗号化のための鍵は公開し，復号のための鍵は秘密にする暗号を**公開鍵暗号**と呼ぶ．公開鍵暗号の実現には代数的手法が全面的に援用されている．ここでは，暗号理論の中でも公開鍵暗号について概説し，暗号理論と代数学との関連について述べる．詳しくは文献 1～3) 等を参照されたい．

2. 公開鍵暗号の概念

共通鍵暗号を用いて暗号通信を行うための準備として，送信者と受信者で同一の鍵を事前に共有する必要がある．この際，秘密裏に鍵を共有せねばならず，どうやって安全に秘密の鍵を共有するかは共通鍵暗号を用いる際のある種のジレンマであり，古くからの問題であった（**鍵共有問題**）．この問題を解決する手法として 1970 年代に提案された暗号が公開鍵暗号と呼ばれるものである．現在では，不特定多数が利用するインターネット上での安全な通信の実現においては，公開鍵暗号は必要不可欠なものとなっている．

公開鍵暗号は共通鍵暗号とは異なり，暗号化に必要となる鍵を公開しているため誰でもその鍵を用いて暗号化を行うことができる．この鍵を公開鍵と呼ぶ．一方で，復号のために用いる鍵は秘密に保持され，これを用いない限り復号できない仕組みとなっている．この鍵を秘密鍵と呼ぶ．一般に，共通鍵暗号のほうが公開鍵暗号に比べて処理速度が速く，サイズの大きなデータ通信には向いている．一方で，共通鍵暗号では事前の鍵共有が必要となるが，それには上述のように公開鍵暗号が有用である．このため，実用的な観点から公開鍵暗号を用いて鍵を事前に共有した後，共通鍵暗号を用いて暗号通信を行うハイブリッド暗号と呼ばれる形で一般的には利用される．

公開鍵暗号の概念は，1976 年に Diffie と Hellman によって提案されたものであり，一方の計算は易しいが逆方向の計算は困難である**一方向性関数**や，さらにある種の秘密を知っていれば，その逆方向の計算が易しくなる**落とし戸つき一方向性関数**の概念と同時に提案されたものである．この（落とし戸つき）一方向性関数の実現に用いられたのが，古くより知られていた計算量的に困難な問題である**素因数分解問題**，**離散対数問題**や**ナップサック問題**等であり，この発見以来現在に至るまで，暗号理論は（計算機を援用する）代数学，特に数論と密接な関係を保ちながら発展してきたと言えよう．それまで数学の中でも実社会への応用

からは最も遠いと考えられてきた数論は，素因数分解問題といった数論の問題に対して効率的なアルゴリズムを見つけるという観点から，直接的に公開鍵暗号の研究と結びついたことにより，突然，現代社会の基盤を支える重要な分野へと変貌してしまったとも言えよう．このような数論の変化について，Fermat 予想の解決で有名な Wiles[4] は次のように述べている：“... One change in number theory over the last twenty years is that it has become an applied subject. (Perhaps one should say it has gone back to being an applied subject as it was more than two thousand years ago. Public key cryptography has changed the way we look at secrecy and codes...)”

3. 一方向性関数と代数的手法

一般的に公開鍵暗号は，鍵生成アルゴリズム $KeyGen$，暗号化アルゴリズム Enc，復号アルゴリズム Dec の 3 つのアルゴリズムの組として表される．受信者は鍵生成アルゴリズム $KeyGen$ にセキュリティパラメータと呼ばれる自然数を入力し，公開鍵と秘密鍵の組 (pk, sk) を得る．pk および暗号化アルゴリズム Enc は公開しておく．暗号文の送信者は伝送されるデータ（これを平文と呼ぶ）を pk と Enc を用いて暗号化して受信者に送る．暗号化関数 Enc は確定的なアルゴリズム，もしくは確率的なアルゴリズムである．確率的なアルゴリズムの場合は平文を暗号化する際，ランダムなビット列を生成し，平文とともに入力として与える．受信者は暗号文を受け取った後，自分しか知りえない秘密鍵 sk を用いて，復号関数 Dec に暗号文と秘密鍵 sk を入力し平文を得る．

公開鍵暗号の実現のためには (落とし戸つき) 一方向性関数を構成しなければならないが，このためにいくつかの代数的手法，特に数論的な問題が主に利用されてきた．理論的に一方向性関数の存在は示されてはいないが，歴史的に有名な計算困難な問題を利用した一方向性関数の候補となるものはいくつか知られている．代表的なものとして，素因数分解問題，有限体上の離散対数問題および有限体上の楕円曲線の有理点のなす群上の離散対数問題（**楕円離散対数問題**）などの数論的な問題がある．

ここで，これらの問題を定義しておく．

[素因数分解問題]　与えられた合成数 n (≥ 2) の非自明な約数 d $(1 < d < n)$ を求めよ．

[有限体上の離散対数問題]　有限体 $\mathbb{F}_q$，$a, b \in \mathbb{F}_q^{\times}$ が与えられているとする．このとき，$b = a^x$ を満たす整数 x が存在すれば求めよ．

[楕円離散対数問題]　有限体 $\mathbb{F}_q$ 上定義された楕円曲線 E，E の 2 つの $\mathbb{F}_q$ 有理点 P，Q が与えられているとする．このとき，$Q = [x](P)$ を満たす整数 x が存在すれば求めよ．

上記の素因数分解問題では，完全な素因数分解ではなく非自明な約数を求めることだけしか要請していないが，素因子の個数は高々 $\log n$ のオーダであり，上記の問題の解法となるアルゴリズムを高々 $\log n$ のオーダ回だけ再帰的に用いることで完全な素因数分解を得ることができる．よって，上記の定義は完全な素因数分解と計算量的に等価な問題とみなせる．また，上記の離散対数問題は，任意の有限群上で定義することができる．

これらの問題は古典的なチューリングマシンモデルに基づく計算困難性が期待されるものであるが，量子計算機と呼ばれる計算機モデルを用いると効率よく解かれてしまうことが数学的に示されている．一方，ナップサック問題に代表される組合せ論的な問題や有限体上の非線形連立方程式を解く問題などは **NP 困難**と呼ばれる問題のクラスに属することが知られており，さらに量子計算機を用いても効率的なアルゴリズムの存在は知られておらず，昨今，これらの問題に基づく公開鍵暗号の研究も盛んである．

一般に，計算困難な問題が与えられても，それを利用した公開鍵暗号を設計することはそう易しいことではなく，落とし戸となる数学的な仕掛けをどう考えるかが重要となる．その数学的な仕掛

けの実現のために，公開鍵暗号研究の初期より，素因数分解問題や有限体上の離散対数問題等が利用されてきたこともあり，鍵生成アルゴリズムに用いるため「与えられた（十分大きな）自然数が素数であるかどうかをいかに判定するか？」という素数判定問題や，暗号の安全性評価のために「与えられた合成数をいかに高速に素因数分解するか？」という素因数分解問題などが暗号における重要な研究テーマとなった．前節の最後で述べたことの繰り返しになるが，これらの問題は，暗号の研究以前から純粋に数論的な興味から研究されてきたものではあったが，あらためて脚光を浴びた形になったと言えよう．特に素数判定問題は，2002 年に Agrawal 等により決定性多項式時間で解けることが示されている．

例えば，次の **Fermat の小定理**およびその一般化である **Euler の定理**は，公開鍵暗号と数論との関連でいえば最も重要な定理である．

定理 1（Fermat） 素数 p, p と互いに素な整数 a に対して，次が成り立つ

$$a^{p-1} \equiv 1 \pmod{p}.$$

定理 2（Euler） 自然数 n, n と互いに素である n 以下の自然数の個数を $\varphi(n)$ とする．n と互いに素な整数 a に対して，次が成り立つ

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

4. 代表的な公開鍵暗号

1976 年の Diffie と Hellman による公開鍵暗号の概念の提案以来，様々な公開鍵暗号が提案されてきた．素因数分解問題の困難性に基づく暗号としては RSA 暗号，Rabin 暗号，Goldwasser–Micali 暗号，Okamoto–Uchiyama 暗号，Paillier 暗号など多数知られている．離散対数問題の困難性に基づく暗号としては有限体の乗法群上の Diffie–Hellman 鍵共有，ElGamal 暗号，Cramer–Shoup 暗号および有限体上の楕円曲線の有理点のなす群上の Diffie–Hellman 鍵共有，ElGamal 暗号，Cramer–Shoup 暗号などが知られている．一方，Merkle–Hellman 暗号や Chor–Rivest 暗号と呼ばれるナップサック問題の困難性に基づく暗号，NTRU 暗号と呼ばれる格子に関する問題の困難性に基づく暗号なども知られている．

ここでは，上記の中からそこで用いられている代数的な仕掛けがそれぞれ異なり，数論的な問題の困難性に基づく方式である RSA 暗号，ElGamal 暗号，Okamoto–Uchiyama 暗号について概説する．

4.1 RSA 暗号

1977 年に Rivest, Shamir, Adleman の 3 人によって提案された公開鍵暗号であり素因数分解問題の困難性に基づく暗号である．RSA 暗号は現在世界中で最も広く利用されている公開鍵暗号である．RSA 暗号は確定的な暗号であり，基本的な形のままで利用することは様々な攻撃に対して脆弱性があることが知られている．そのため，RSA-OAEP（RSA-Optimal Asymmetric Encryption Padding）といった乱数を用いたある種のパディングを用いて，適応的選択暗号文攻撃といった強力な攻撃法に対して強秘匿性という高い安全性を持つ暗号へと変形された形で利用されている．

[鍵生成] セキュリティパラメータ k に対し，それぞれ k ビットの 2 つの異なる奇素数 p, q を生成し，$n = pq$ を計算する．このとき，合成数 n の素因数分解が十分に困難であるように k の大きさを選ぶ必要がある．また，$L = \varphi(n) = (p-1)(q-1)$ を求め，L 以下の適当な自然数 e を L と互いに素となるように選び，$ed \equiv 1 \pmod{L}$ を満たす d を求める．公開鍵 pk および秘密鍵 sk として $pk = (n, e)$, $sk = d$ を出力する．復号の効率化にあたって，p, q それぞれを法とした演算を利用することもあり，$sk = (d, p, q)$ とすることもある．また，$\varphi(n)$ の代わりに $p-1$ と $q-1$ の最小公倍数を L としても良い．

[暗号化] 平文 m（n 以下の自然数）を入力とし，次で暗号化して暗号文 c を得る．

$$c = m^e \bmod n.$$

ここで，$m^e \bmod n$ は m^e を n で割った剰余（0

以上 $m-1$ 以下）とする．

[復号]　暗号文 c を入力とし，次で復号して平文 m を得る．

$$m = c^d \bmod n.$$

復号が正しく行われることは，Euler の定理による．

4.2 ElGamal 暗号

1984 年に ElGamal によって提案された公開鍵暗号であり，Diffie–Hellman 鍵共有方式の変形である．有限体の乗法群や有限体上の楕円曲線の有理点のなす群上で実現できる．ここでは，一般的な有限群（演算は乗法的に記す）を用いた形で述べる．ただし，「与えられた位数を持つ有限群が効率よく生成できる」，「その群の位数が十分大きいとき，その群上の離散対数問題が十分に困難である」，「平文が効率よくその有限群の要素として表現できる」等の条件は満たしているとする．

[鍵生成]　セキュリティパラメータ k に対し，k ビットの奇素数 l を生成し，位数 l の群 G およびその 1 つの生成元 g を生成する．このとき，位数 l の群 G 上の離散対数問題が十分に困難であるように k の大きさを選ぶ必要がある．次に，1 以上 l 以下の自然数 x をランダムに選び，$y = g^x$ とする．秘密鍵，公開鍵として，$pk = (l, y, G, g)$，$sk = x$ を出力する．

[暗号化]　1 以上 l 以下の自然数 r をランダムに選び，平文 $m \in G$ を次で暗号化して暗号文 $c = (c_1, c_2)$ を得る．

$$c_1 = m \cdot y^r, \quad c_2 = g^r.$$

[復号]　暗号文 $c = (c_1, c_2)$ を入力とし，次で復号して平文 m を得る．

$$m = c_1 \cdot c_2^{l-x}.$$

復号が正しく行われることは，$y^r \cdot (g^r)^{l-x} = 1_G$（$1_G$ は G の単位元）が成り立つことからわかる．

4.3 Okamoto–Uchiyama 暗号

1998 年に岡本龍明と筆者によって提案された公開鍵暗号であり素因数分解問題の困難性に基づく暗号である．受動的攻撃に対する安全性が素因数

分解問題が計算量的に困難であるということと等価であることが数学的に証明されているものである．RSA 暗号とは公開鍵で用いられている合成数の形が異なり，$n = p^2q$ という形をしているが，本質的にどちらの形が素因数分解するのが困難なのかはまだよくわかっていない．RSA 暗号と同様に乱数を用いたある種のパディングを用いて，適応的選択暗号文攻撃といった強力な攻撃法に対して強秘匿性という高い安全性を持つ暗号へと変形された方式も存在する．

[鍵生成] セキュリティパラメータ k に対し，それぞれ k ビットの 2 つの異なる奇素数 p, q を生成し，$n = p^2q$ を計算する．このとき，合成数 n の素因数分解が十分に困難であるように k の大きさを選ぶ必要がある．また，n 以下で n と互いに素である自然数 g の中で $g^{p-1} \not\equiv 1 \pmod{p^2}$ となるものを選ぶ．さらに，$h = g^n \bmod n$ とする．公開鍵 pk および秘密鍵 sk として $pk = (n, g, k, h)$, $sk = p$ を出力する．

[暗号化] 平文 m（$0 \le m < 2^{k-1}$ となる整数）および n 以下で n と互いに素である自然数 r をランダムに選び，(m, r) を入力とし，次で暗号化して暗号文 c を得る．

$$c = g^m h^r \bmod n.$$

[復号] 暗号文 c を入力とし，次で復号して平文 m を得る．

$$m = L(c_p)/L(g_p) \bmod p.$$

但し

$$g_p = g^{p-1} \bmod p^2, \quad c_p = c^{p-1} \bmod p^2,$$

および $L(x) = (x-1)/p$ とする．

復号が正しく行われることは，復号で用いられる関数 L の持つ準同型性

$$L(xy) \equiv L(x) + L(y) \pmod{p}$$

（$x, y \in \mathbb{Z}, x, y \equiv 1 \pmod{p}$），つまり，関数 L が対数関数のように振る舞うことによる．この関数 L は Fermat 商と呼ばれることもあり，本質的には局所体の数論で扱われる p 進対数関数とみなせる．この関数 L を用いることで，$(\mathbb{Z}/p^2\mathbb{Z})^\times$ の p-Sylow 部分群上の離散対数問題が効率よく解けることがわかる．$c_p = g_p^m \bmod p^2$ より $L(c_p) = mL(g_p) \bmod p$ となり，$L(g_p) \not\equiv 0 \pmod{p}$ であるので，$m = L(c_p)/L(g_p) \bmod p$ が示せる．

5. その他の代数的手法

ここでは，上で述べたものとは異なる暗号に関連する代数的手法（格子暗号，多変数公開鍵暗号）について概説する．

5.1 格子に関する問題と暗号

m, n を自然数（$m \ge n$）として，m 次元ユークリッド空間 $\mathbb{R}^m$ における格子とは，$\mathbb{R}^m$ の n 個の線形独立なベクトル $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ の整数係数の線形結合の集合

$$\mathcal{L}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) = \left\{ \sum_{i=1}^{n} x_i \boldsymbol{b}_i \;\middle|\; x_i \in \mathbb{Z} \right\}$$

のことを言う．$\boldsymbol{B} = [\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n]$ として $\mathcal{L}(\boldsymbol{B})$ 等とも書く．n は格子の次元または階数と呼ばれる．格子はユークリッド空間内の疎な加法部分群として特徴づけられるが，非常に豊富な組合せ的構造を持ち，様々な分野に現れる重要な対象であり，多くの応用を持つ．公開鍵暗号への応用としては，その実現のための落とし戸の構成および攻撃（安全性評価）の両方に利用される．

格子は疎であるため，Euclid ノルム $||\cdot||$ に関する最短の非零ベクトルを含む．このベクトルのノルムを，第 1 次最小と呼び $\lambda_1(\mathcal{L})$ または $||\mathcal{L}||$ などと書く．格子に関する最も有名な問題は，与えられた格子 $\mathcal{L}(\boldsymbol{B})$ の中の $\lambda_1(\mathcal{L})$ の長さを持つベクトルを求める問題であり，**最短ベクトル問題**（Shortest Vector Problem, SVP）と呼ばれる．

> **[最短ベクトル問題，SVP]** 基底 $\boldsymbol{B} \in \mathbb{Z}^{m \times n}$ が与えられたとき，$\boldsymbol{0}$ でないベクトル $\boldsymbol{Bx}$（但し，$\boldsymbol{x} \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}$）で，任意の $\boldsymbol{y} \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}$ に対して $||\boldsymbol{Bx}|| \le ||\boldsymbol{By}||$ となるものを求めよ．

最短ベクトル問題と同様に，**最近ベクトル問題**（Closest Vector Problem, CVP）と呼ばれる問

題等も定義できる．

最短ベクトル問題や最近ベクトル問題を解く多項式時間アルゴリズムは現在までのところ知られておらず，CVP は NP 困難，SVP もランダム帰着の下で NP 困難であることが示されている．素因数分解等の数論的な問題と異なり，格子に関連する問題は量子計算機による効率的なアルゴリズムは存在しないのではないかと期待されている．

これらの問題を解くことが非常に困難であるため，より扱いやすい，最適解そのものではなくある指定した定数 γ 倍の範囲内にあることだけが保証される解を求める，近似的に解く問題も考察されるようになった．

> **[近似 SVP]**　定数 $\gamma > 0$，基底 $\boldsymbol{B} \in \mathbb{Z}^{m\times n}$ が与えられたとき，$\boldsymbol{0}$ でないベクトル $\boldsymbol{Bx}$（但し，$\boldsymbol{x} \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}$）で，任意の $\boldsymbol{y} \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}$ に対して $||\boldsymbol{Bx}|| \leq \gamma \cdot ||\boldsymbol{By}||$ となるものを求めよ．

同様にして近似 CVP も定義できる．

2 次元の場合の SVP は Gauss によって提案されたアルゴリズムを用いて多項式時間で解くことができる．しかし，次元が高くなると一般には指数時間アルゴリズムしか知られていない．一方，近似的問題においては，一般の次元における近似 SVP を解くアルゴリズムとして Lenstra, Lenstra, Lovász による基底簡約アルゴリズム，いわゆる **LLL アルゴリズム**が有名である．これは，Gauss のアルゴリズムの一般化とみなせるものである．基底簡約アルゴリズムは，格子基底を入力とし，十分短い長さのベクトルからなる基底を出力する多項式時間アルゴリズムである．LLL アルゴリズムは，数学や計算理論の分野において非常に多くの応用を持ち，特に，暗号との関連では，ナップサック問題に基づく暗号方式への攻撃法として最も有効な方法として用いられてきた．

一方，1990 年代後半の Ajtai による格子の問題の計算量に関する一連の仕事は，ある種の格子の問題における最悪の場合と平均の場合の計算量の間の興味深い関係に関するものである．さらに，Ajtai は SVP が NP 困難であることを，ランダム帰着の下で証明した．SVP が NP 困難であることを示すことは，長年の未解決問題であった．これらの計算量的結果に基づき，いくつかの格子の問題の困難性に基づく暗号方式が提案されており，これらの方式の中の 1 つである Ajtai–Dwork による暗号方式は，基づく問題が，最悪の場合の困難さと平均の場合の困難さが等価であるため，最悪の場合に基づく安全性証明を与えることができるという驚くべき特徴を持つ．

5.2 多変数公開鍵暗号

有限体係数の非線形多変数連立方程式を解く問題は，NP 困難な問題として知られている．格子の問題等と同様に，量子計算機を用いても効率的なアルゴリズムは存在しないと考えられているため，この問題に基づく公開鍵暗号は耐量子計算機暗号として期待されている．代表的なものに，1988 年に提案された松本–今井暗号と呼ばれる暗号方式がある．非線形多変数連立方程式を解くことが困難であることに安全性の根拠をおいている暗号方式は**多変数公開鍵暗号**（Multivariate Public-Key Cryptosystems, MPKC）と呼ばれる．MPKC には，多項式環におけるイデアルの生成多項式系（基底と呼ばれる）の共通零点を求めることが安全性解析（攻撃）となり，共通零点を求めるには，何らかの意味でイデアルの「良い」基底があれば有効である．この 1 つの特徴づけとして Gröbner 基底がある．多変数公開鍵暗号への攻撃手法として，この Gröbner 基底を求めるアルゴリズムが一般的であり最も強力である．多変数公開鍵暗号の研究では，代数幾何学的手法が重要となる．

2004 年に秋山浩一郎と後藤泰宏により提案された代数曲面暗号（Algebraic Suface Public-Key Cryptosystems, ASC）と呼ばれるものがある．これは有限体上定義された代数曲面上の非自明なセクションを求める問題（求セクション問題）に安全性の根拠をおくもので，非常に興味深いものであったが，ASC04 と呼ばれる方式に対して，2007 年に徳永浩雄と筆者により Gröbner 基底に関する基本的な性質に基づく効率的な攻撃法が提案されている．この攻撃法は当初はアルゴリズムの部分

正当性の証明に，ある条件が仮定されていたが，その後，条件はなくなり一般化されている．この安全性解析の研究は Gröbner 基底の計算アルゴリズムが多変数公開鍵暗号の安全性解析に有効に働いた１つの例である．

6. おわりに

現在盛んに研究されている楕円曲線および代数曲線を用いた暗号等については紙数の関係もあり今回は触れることはできなかったが，数論的手法を中心に様々な代数的手法が暗号の研究で生かされていることの一部は紹介できたと思う．本稿の最後に，多変数公開鍵暗号に対する公開鍵暗号の提案者の一人である Diffie[5] の言葉を引用し，今後も，代数的な手法に限らず様々な数学が暗号研究と出会い互いに発展していくことを期待したい：

"Mathematically speaking, the security of RSA-type cryptosystems relies on the complexity of integer factorization and is based on results in number theory developed in 17th and 18th centuries. Elliptic curve cryptosystems employ the use of mathematics from the 19th century. Multivariate cryptography goes one step further, using results in algebraic geometry developed in the 20th century."

参考文献

1) 森山大輔，西巻陵，岡本龍明，『公開鍵暗号の数理』，共立出版 (2011).
2) N. コブリッツ（林彬訳），『暗号の代数理論』，丸善出版 (1999).
3) J.A. ブーフマン（林芳樹訳），『暗号理論入門』（原書第３版），丸善出版 (2007).
4) A. Wiles, *Twenty Years of Number Theory, Mathematics: Frontiers and Perspectives*, AMS, pp.329–342 (2000).
5) J. Ding, J.E. Gover and D.S. Schmidt, *Multivariate Publilc Key Cryptosystems*, Springer (2006).

（うちやま・しげのり，首都大学東京大学院理工学研究科）

粗視化とスケール変換

生命現象へのアプローチ



加藤　毅

1. Introduction

生命現象は，DNA や様々な種類のタンパク質どうしが複雑にからみ合いながらある部位のネットワークを構成し，さらにそれら局所的なネットワークどうしが相互作用して大域的なネットワークを構成している．分子細胞生物学と言っても非常に裾野が広く，むしろその広さが生物学ゆえんとも言える．各テーマごとにその個性を追求するための独自の切り口を持っており，一方でそれら総合体によって構成されるメカニズムが，例えばマクロにおいて魚やシマウマの縞模様のようなパターンを生じさせている．数理的手法も，微分方程式のみならずテーマごとに相性に応じて様々な数学が用いられてきている．例えばシグナル伝達では情報理論，皮膚の模様など周期的な構造に対しては拡散方程式，またタンパク質の位相的な構造解析にはリーマン面のモジュライ理論に現れるファットグラフを用いる理論，遺伝子などのネットワークに対してはグラフ理論など，一見するとばらばらな手法が用いられている．それら広大なテーマをすべて統一して扱うことは不可能に見えるが，一方で生物のある側面をテーマにしている限りそれぞれどこかでつながっているはずである．複数のコアなテーマをある程度融合することで，統一的に理解を深めていくことが可能なのではないか．そこへの第一歩として，数理解析研究所共同研究「離散力学系の分子細胞生物学への応用数理」を理研 CDB の上田泰己さん（現東大医学部）と共同で開催したことがあり，そこでは生命数理においてコアになると考えられる 6 つのテーマを選んだ．もちろんそれ以外にも重要なテーマはあるが，選んだものだけでも，すでにそこには広大な領域の数理が現れた．しかしそのような様々な数理の手法を同時にまた直接的に適用することはあまりに複雑になってしまう．その解決には，個別に用いられている数理的手法を，より抽象化してその枠組みを取り出すことが一つの方向性を与えるのではなかろうか．それにより個別のテーマに対して得られる情報は減るが，それぞれの数理的手法の架け橋をつくっていくことができるであろう．ここでは，特にスケール変換による粗視化によって，数理的手法の枠組みを取り出す試みを取り上げる．

代謝や遺伝子ネットワークなど，複数の元が相互に作用してある種の系を構成しているとき，最も抽象的に言えば何か初期値を与えればそれに反応した結果としての値が検出される．その系を表現する空間を与えることができれば，その反応は空間の間の写像 $f : X \to X$ としてとらえることができる．例えば DNA や RNA，タンパク質などは有限個のアルファベットからなるワードで与えられ，それらの集合で構成される対象が X であり転写や酵素としての機能が f である．ここでは生命現象のうち普遍的に現れる特徴的な性質を取り上げ，ある側面に対してそれらと適合するまたは構造の類似性を持つ数学について概説をする．そ

れらが直接応用され得ることは必ずしも期待していないが，生命現象に現れる構造を数理を用いて理解するためのヒントになる可能性があると筆者は考えている．

2. シグナル伝達と記号力学系

シグナル伝達は外部からの刺激を，細胞膜に存在する受容体を介して細胞内部に伝達する機能である．個別の物質としての個性に依存した情報を変換して，タンパク質などのネットワークに信号を伝えるのであるが，その一般的な原理は符号化によりアルファベットの有限列からなるワードを，別のものに置き換える操作として表現される．ワードで情報を表す場合，アルファベットの数と各ワードの長さに応じてその複雑性が決まる．どちらもできるだけ少ないまたは短いほうがより効率的だが，やりすぎると情報を復元できなくなる．両者の「適切なサイズ」に関する評価は情報エントロピーの基本理論で扱われており，例えば情報が復元できるためには，平均のワードの長さと，アルファベットの数のログをかけたものが，情報エントロピーの値よりも大きくなる必要がある．生命は実に多くのシグナルを受信や発信することで情報の伝達を行っているが，限られた数の分子やネットワークシステムを用いてどのような応答を行っているのだろうか．細胞は時間情報コードと呼ばれる，分子の時間変化に情報を刻むことで通信処理を行っているという．すると，ネットワークの局所的な構造がその大域的な構造に対して伝達機能を果たしていることになる．

人の周期が 24 時間なのは地球の自転にあわせたことによるが，それは人特有のものではなくほとんどの生体内が持つ特性で体内時計と呼ばれている．昼夜変化のない環境で 1 日周期の活動が変化するリズムが，植物や多くの動物や単細胞生物に共通してみられる生命の普遍的機能であり，それは生命ネットワークの周期性といえる．周期は 24 時間ぴったりではなくだいたい 22 から 27 時間の幅があることから概日リズムと呼ばれている．多くの人が 24 時間周期で生活しているのは，昼夜の光シグナルを受けて 24 時間に同調しているからで，「だいたい 24 時間」の周期をもつが外界からの刺激で 24 時間ぴったりになるように調節されている．

3. 周期について

一般に，空間 X 上に写像 $f : X \to X$ が与えられたとき，その特性を調べることを考える．最初に考えるべき性質は，$f(x) = x$ となる**固定点** $x \in X$ や，$f^n(x) \equiv f \circ \cdots \circ f(x) = x$ となる**周期点**が存在するか，ということであろう．そのためには X や f の特徴をある程度理解する必要があるが，ある状況では X の性質だけから f に関する情報を引き出すことができる．$D \subset \mathbb{R}^n$ を単位円盤とする．**ブラウアーの固定点定理**とは，

定理： $f : D \to D$ を連続写像とするとき，f には必ず固定点が存在する．

これは空間としての円盤が非常に単純な構造をしていることの帰結であるが，f に緩い条件しか与えていない状況で成立する非常に一般的な性質である．一方で，理論的に固定点の存在がわかっていることと，具体的にその点を求めることは全く別のことであることにも注意が必要である．別の例を見てみよう．X を多様体としその上のベクトル場 V が与えられると，それを「積分」することで X 上の微分同相写像 $f : X \cong X$ が得られる．f の固定点は $V(p) = 0$ となるベクトル場の 0 点と一致するが，逆に固定点が存在しない状況を考えてみる．それはすべての $p \in X$ に対して $V(p) \neq 0$ となるような，至る所 0 とはならないベクトル場が存在するか，という問いである．

定理： n 次元球面上に至る所 0 ではないベクトル場が存在するのは，n が奇数の場合のみに限り，逆に奇数の場合に存在する．

至る所 0 ではないベクトル場を少し変形してもその性質は保たれるし，また地球の自転は北極と

南極に固定点が存在しており，それをどのように変形しても固定点をなくすことはできない．2 つの例はどちらも代数的位相幾何学のアイデアが背景にあり，写像の小変形では変わらない安定した性質を保証しているが，一方でどちらも厳密な周期性に関する性質を扱っており，「ほぼ周期的」な性質に関しては情報を与えるものではない．

体内時計は生体内に複数存在しており，例えば哺乳類の場合には，脳に体内時計のセンターとして働く時計が存在して，一方で身体の様々な部分に細胞単位で時計があり，それぞれの時計細胞が概日リズムを刻みながら，他の時計細胞のリズムと同調することによって，個体全体としてのリズムを作り出していることが知られている．真夜中に強い光を浴びると体内時計が一時的に停止する Singularity 現象が起こるが，各細胞の時計の状態（位相）がバラバラになって互いのリズムを打ち消し合い，細胞集団全体としては概日リズムの振幅がほぼ平坦に見えてしまうことによって起こることが最近実証された．

概日リズムのような「だいたい周期的」な振舞いをしたり，またほかのネットワークからの多少の干渉にも耐えながらだいたい周期的な状態を維持することが可能だが，大きな摂動によりだいたい周期性が壊れてしまう，そのような性質は数学ではどのようなもので扱えるだろうか．

4. トロピカル幾何学による粗視化について

紙の上に実数直線とその上の整数点の集合

$$\mathbb{Z}=\{\dots,-l,\dots,-1,0,1,2,\dots,k,\dots\}\subset\mathbb{R}$$

を書いてみると，そのまま見れば双方は互いに異なる対象だが，その紙をだんだん遠くに引き離して見てみることで，十分大きな N に対して，

$$\frac{1}{N}\mathbb{Z}\equiv\left\{\dots,-\frac{1}{N},0,\frac{1}{N},\dots,\frac{k}{N},\dots\right\}\subset\mathbb{R}$$

のように格子点上の間隔が狭く見えてきて，だんだん実数直線に「近く」見えてくるようになる．そのように整数点と実数直線とは互いに「ある種の構造類似性」があると言え一種のスケール変換と言える．ここでは**トロピカル幾何学**と呼ばれるスケール変換を扱うことにする[2,5]．

$t>1$ をパラメーターとし $\bar{z}^{j_l}=z_1^{j_l^1}\dots z^{j_l^n}$ とおくとき，トロピカル幾何学では，

$$F_t(\bar{z})=\left(\sum_{l=1}^{m}t^{\alpha_l}\cdot\bar{z}^{j_l}\right)\left(\sum_{l=1}^{m'}t^{\beta_l}\cdot\bar{z}^{j'_l}\right)^{-1}$$

の形の有理関数を考える．これは，$\bar{z}=(z_1,\dots,z_n)$ の各成分を正の数に取れば値も正の数になる．パラメーターを $t\to\infty$ とスケール変換することにより，その極限関数として以下のものが得られる．

$$\varphi(\bar{x})=\max(\alpha_1+j_1\bar{x},\dots,\alpha_m+j_m\bar{x})$$
$$-\max(\beta_1+j'_1\bar{x},\dots,\beta_{m'}+j'_{m'}\bar{x}).$$

両者の関数は，α,β,j などの係数を決めれば，関数の表示は互いに一意に定まり，それをトロピカル対応と呼ぶことにする．

具体例で考察する．$\varphi(x_0,x_1)=\max(0,x_1)-x_0$ とすると，$\max(0,x_1)\geq 0$ が常に満たされるので，表示は違うが関数としては同じものが得られる．

$$\psi(x_0,x_1)=\max(\varphi(x_0,x_1),-x_0)=\varphi(x_0,x_1).$$

対応する有理関数は，φ に対しては $F_t(z_0,z_1)=(1+z_1)\frac{1}{z_0}$ となり，ψ は $G(z_0,z_1)=(2+z_1)\frac{1}{z_0}$ で関数として互いに異なるが，F と G は無限遠方での振舞いが同じであることが分かる．

φ と ψ をそれぞれ $(\max,+)$ 関数とし，トロピカル対応でそれぞれ F_t と G_t を与えるとする．φ と ψ が関数として同じものであるとき，F_t と G_t が互いに**トロピカル同値**と呼ぶことにする．

5. 再帰写像について

初期条件 $\bar{x}_0=(x_0,\dots,x_{n-1})\in\mathbb{R}^n$ をとり，

$$x_N=\varphi(x_{N-n},x_{N-n+1},\dots,x_{N-1})$$

で帰納的に軌道を定める．x_{n+1} や x_{n+2} を書き下してみると，この軌道を決めるためには写像 φ を何度も合成した値を知る必要があることがわかり，その軌道はとても複雑な振舞いをしそうである．

初期値 $\bar{z}=(z_0,\dots,z_{n-1})\in\mathbb{R}^n_{>0}$ を，$x_0=\log_t z_0,\dots,x_{n-1}=\log_t z_{n-1}$ とおいて，同じルー

ルで F_t の軌道を

$$z_N = F_t(z_{N-n}, z_{N-n+1}, \ldots, z_{N-1})$$

とおくと，$\log_t z_N$ は，$t \to \infty$ で x_N にある意味で漸近的に収束することがわかり，「F_t による軌道の無限遠方に φ による軌道が乗っている」ようなスケール変換を与えている．

実は一般にトロピカル同値なものによる軌道どうしは，初期値によらない一様評価が成り立つことが分かっている．

任意の初期値 $(x_0, \ldots, x_{n-1})$ について，その軌道 $\{x_N\}_N$ が $x_N = x_{N+M}$ をすべての N について満たすとき，φ は周期 M の再帰写像であるという．F_t についても同様に再帰性が考えられる．上の例で $\varphi(x_0, x_1) = \max(0, x_1) - x_0$ は周期 5 の再帰写像で，$F_t(z_0, z_1) = (1 + z_1)\frac{1}{z_0}$ も周期 5 の再帰写像になる．

さて，F_t が再帰写像であるとき，F_t とトロピカル同値な G_t もまた再帰写像になるであろうか．上の例で，ψ に対応する $G_t = (2 + z_1)\frac{1}{z_0}$ は F_t とトロピカル同値になるが，実は G_t は再帰写像にはならない．つまり再帰性はトロピカル同値では保たれない性質である．しかしそれでも無限遠方での振舞いが同じであるからには，何か共通の構造を持っているはずである．

F_t が周期 M の**擬再帰写像**とは，ある定数 $C \geq 1$ が存在して，任意の初期値 $z_0 \ldots, z_{n-1}$ に対してその軌道を $\{z_N\}_N$ とおくとき，N によらない以下の一様評価が成り立つときをいう．

$$\frac{z_{M+N}}{z_N}, \ \frac{z_N}{z_{N+M}} \ \leq C.$$

再帰性は $C = 1$ と同値であり，特に再帰写像は擬再帰性を満たす．

定理：φ と F_t がトロピカル対応であるとき，φ が周期 M の再帰写像であることと，F_t が周期 M の擬再帰写像であることは同値である．

これにより，有理関数で「だいたい周期的」な振舞いをすれば，無限遠方では周期的になることがわかる．

また軌道は表示によらずに関数の値のみに依存するので，擬再帰性はトロピカル同値類で不変な性質であることもわかる．例えば，φ と φ' が不等式 $\varphi \geq \varphi'$ を満たすとする．対応する有理写像をそれぞれ F_t と H_t とおくと，$G_t = F_t + H_t$ は F_t とトロピカル同値になるので，F_t が擬再帰であれば G_t も同じ性質を持つ．

さて，体内時計の話題に戻って，擬再帰性を「だいたい周期的」な振舞いをしていると見なせば，トロピカル同値性を保ちながら有理関数を変形してもだいたい周期的な状態は維持される．一方でトロピカル同値性を超えるような摂動を加えてそのクラスからはみ出てしまえば，もはやだいたい周期性が壊れてしまう．例えば，不等式 $\varphi \geq \varphi'$ を満たさないものに対しては，$F_t + H_t$ はもはや擬再帰性は持ち得ない．

ここで重要なことは，だいたい周期的な振舞いをする有理関数は，その無限遠方において周期性を保証するような拘束条件が与えられていることで，このような枠組みをもっているがゆえに，その振舞いが可能になることである．

6. Turing の拡散方程式と皮膚の模様

魚やキリンなどの皮膚の模様は等間隔の繰り返しパターンをつくっていて，それらはある種の波であることが理解されている．Turing が導入した拡散方程式

$$\frac{du}{dt} = f(u, v) + c_1\Delta(u), \quad \frac{dv}{dt} = g(u, v) + c_2\Delta(v)$$

では，u と v はそれぞれ 2 種類の分子の濃度を表していて，u は濃度依存的に自分自身と v の合成を促進して，v はその逆の役割を果たしている．それにより物質の濃度分布が均一にならずに，濃い部分と薄い部分が空間に繰り返しパターンをつくって安定することにより，その波ができる仕組みである．その際係数 c_1 と c_2 の大小関係に大きく依存して，全く異なるパターンを形成する．Turing の拡散方程式も離散化されトロピカル幾何学によりオートマトンに還元されており，その研究も現在行われている．

パターンに関連して，形態形成においては，ある種の分子の濃度勾配の変化によりパターンが誘導されていく．また複数のあるタンパク質の発現振動に応じて，神経幹細胞の自己複製や，異なる細胞分化を誘導する現象がある．

パラメーターが変化することで，全く異なるダイナミックスが得られるようなものが，トロピカル幾何学においても得られることを以下で見てみる．$F(z_0, z_1) = (1 + z_1)\frac{1}{z_0}$ は周期 5 の再帰写像だから特にすべての軌道は有界．$F_l(z_0, z_1) = \frac{1+l+z_1}{z_0}$ は，すべての $l = 0, 1, \ldots$ について f とトロピカル同値になるが，各 F_l, $l \geq 1$ に対してすべての軌道が有界かどうかは今のところわかっていない．

そこで摂動をしてみる．十分小さい正の数 $\epsilon_0 > 0$ を固定し，$-\epsilon_0 < \epsilon < \epsilon_0$ とする．F_ϵ を $F = F_0$ の連続な摂動とする．F が F_ϵ について**停留**しているとは，ある定数 $C > 0$ が存在して，任意の初期値 $\bar{z}_0$ であってその長さが C 以上のものの軌道について，以下の 2 つの性質を持つときを言う．

(1) 任意の小さい正の数 $\epsilon > 0$ について，F_ϵ の任意の軌道は有界．

(2) 任意の小さい負の数 $\epsilon < 0$ について，F_ϵ の任意の軌道は非有界．

定理：$G_t(z_0, z_1)$ を $F(z_0, z_1) = \frac{1+z_1}{z_0}$ とトロピカル同値とする．このとき $(G_t)_\epsilon(z_0, z_1) = z_0^\epsilon G_t(z_0, z_1)$ について G_t は停留している．

このことは，対応する $\varphi_\epsilon(x_0, x_1) = \max(0, x_1) - x_0 + \epsilon x_0$ に対する軌道について，$\epsilon > 0$ では可縮な力学系になっており，$\epsilon < 0$ では拡大するものになっていることから従う．

7. 粗視化による構造類似性の発見

魚や蛇の骨は周期的な構造をしている．近年，皮膚の縞模様に現れる Turing パターンが，皮膚の模様とは一見全く異なる骨の形態形成のメカニズムにも存在していることがわかってきた．皮膚の模様と骨の形とは，それぞれ全く異なる対象にも関わらず，そこに現れるメカニズムの枠組みに

構造類似点が見つかったことになる．

一見全く異なる2つの数学の対象が，粗視化によりそれら枠組みの構造類似性を持つ例を以下で紹介する[2,4]．

孤立波を記述する**KdV方程式**は，非線形方程式の中でもとりわけ重要な数理物理学の対象としてこれまで研究されてきた．それが幾何学的群論に現れる**ランプライター群**と関係があることを以下で見てみる．KdV方程式

$$\frac{\partial u}{\partial t} + 6u\frac{\partial u}{\partial x} + \frac{\partial^3 u}{\partial x^3} = 0$$

は，非線形方程式であるため一般解については直接解析することは易しくはないが，方程式を離散化することで計算機による解析が可能になる．離散KdV方程式は以下のもので与えられる．

$$\frac{1}{u_n^{(t+1)}} - \frac{1}{u_n^{(t)}} = \frac{\delta}{1+\delta}(u_{n+1}^{(t+1)} - u_{n-1}^{(t)}).$$

それをトロピカル幾何学によるスケール変換を施すことで，離散方程式から次の**箱玉系**（Box-Ball System, BBS）

$$B_k^{(j+1)} = \min\left(1 - B_k^{(j)}, \sum_{\mu=-\infty}^{k-1}(B_\mu^{(j)} - B_\mu^{(j+1)})\right)$$

が得られる．その力学系は以下の図のように表される．

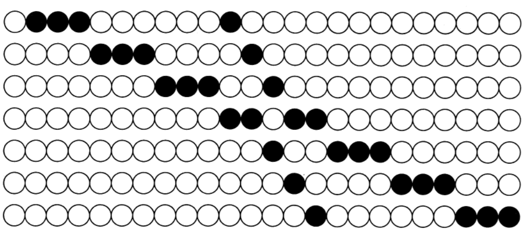
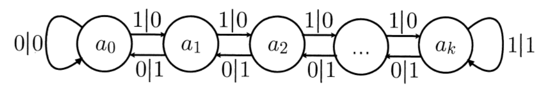


図1　BBS.

両無限格子上に有限個のボールが置かれており，それらは黒丸で表示され，箱玉系はそれらの時間発展を表す．黒塗りのボールが連続して現れたほうがスピードが早くなり，ある時刻には3つ連続した黒塗りのボールが，もともとそれより右にあった1つの黒塗りボールに追いつき，相互作用してのちに，今度は1つの黒塗りボールを3つ連続した黒塗りのボールが追い越すことになる．ソリトンに対応させてみれば，連続した黒塗りボールの数が波の高さに相当する．

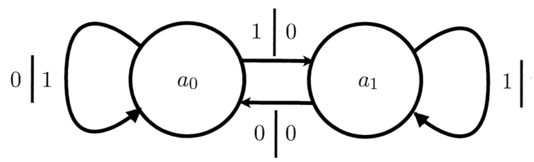
箱玉系は，次のオートマトン図式で $k \to \infty$ としたもので与えられる．



状態の数が有限なものは，運搬車付き箱玉系と呼ばれ BBS_k と書く．そのうち最も簡単なものは $k = 1$ のものである．

さて幾何学的群論において，一般に有限生成群に対してその生成元を与えると，対応してケーリーグラフと呼ばれる（無限）グラフが与えられる．その上のランダムウォークに深く関係する**変換作用素**が $M = 1 + \Delta$ として得られる．

一般に根付無限樹木に作用する有限生成群の場合，変換作用素は有限次元対称行列の無限列 $\{M_n\}_n$ で与えられ，各レベルでの行列は次のステップのそれとはある種の入れ子構造をなしている．ランプライター群のオートマトン図式は以下で与えられる．



これは BBS_1 と形が良く似ているが，実際には BBS_1 は可逆ではないため群構造を持たず，力学系としての構造は異なる．

さて，オートマトンで与えられる力学系はBBSなど一般には可逆な作用ではないが，変換作用素の無限列が同じ構成で与えられる．無限個存在する固有値の分布をそれぞれ調べてみると，以下の事実が分かった．

定理：ランプライター群オートマトンの変換関数のスペクトル分布は，BBS_1 のそれと一致する．

非線形偏微分方程式のような，もともと複雑な構造をもつ対象について，ある側面（この場合はその力学系）についての構造の枠組みを取り出すことで，それとは全く異なるように見える対象との間に**スペクトル構造類似性**を共有していること

を見出すことができた．

8. 終わりに

生命現象に現れるネットワークの特性は個々の状況に応じて異なり，対応して適合する数理的手法も異なる．生命現象を統一的に扱うことができるのかどうか，少なくとも現段階でそれを実行しようとすれば複数の数理的手法を同時に扱う必要が出てくる．そのためには，一度に扱う手法の数が多すぎることなく，人の脳が許容可能なキャパシティー内で理論を構成する必要があろう．最近，比較的シンプルな構造を持つ生命の神経系をまるごと観測してしまおうというプロジェクトがあると聞いた．その手法自体は人のような複雑な構造を持つ生命には直接適用できないであろう．そもそも「人の数理」によって自分自身を客観的にとらえることは不可能のように筆者には思える．しかしそれでも比較的シンプルな構造を持つ生命に対するまるごと手法の枠組みが，ある種の体系的な数理生命理論構成への架け橋となれば大変すばらしいことである．

ここで述べた生命現象に関しては参考文献 1, 3) を，さらに CREST 領域「生命動態の理解と制御のための基盤技術の創出」のホームページの，各研究チームの紹介欄を挙げておく．また 1, 3, 5) については京都大学学術情報レポジトリー KURENAI（http://repository.kulib.kyoto-u.ac.jp）から見ることができる．

参考文献

1) 「数学者のための分子生物学入門」VOL.1–VOL.5, 2003, 2004, 2006, 2007（物性研究 **81-1**, (VOL.1); **85-1** (VOL.3); **87-3** (VOL.4)).
2) 「ランダムから可積分系へ：スケール変換によるパターン形成」東北大学春の学校 (2007).
3) 「離散力学系の分子細胞生物学への応用数理」数理解析研究所講究録 **1698** (2010).
4) T. Kato, S. Tsujimoto and A. Zuk, *Spectral coincidence of transition operators, automata groups and BBS in tropical geometry*, to appear.
5) 加藤　毅,「実有理力学系とトロピカル幾何学」, 日本数学会企画特別講演 (2009).

（かとう・つよし，京都大学大学院理学研究科）

代数学の展望

代数学はいかに応用されるだろうか

宮西　正宜

現在，最もよく知られている代数学の応用は，多項式環イデアルのグレブナー基底，巨大素数や有限群の離散対数を用いた暗号理論，それに代数曲線や代数曲面などの有理点や因子などを用いた代数幾何学符号（Goppa Code）などであろう．古典的な 0 と 1 の連鎖で表される符号理論そのものが標数 2 の基礎体上のベクトル空間の理論の上に成立している．

有限生成多項式環のイデアルは有限個の元で生成されることはヒルベルトによって証明されている．具体的な生成系を見出すことは必ずしも簡単ではないが，イデアルの（背景にある問題に沿った）最適な有限生成系を見つける必要がある．ブッフベルガーは先生であるグレブナーのアイデアに基づいて，単項式順序とそれによるイニシアル・イデアルという概念を入れて基底を求める方法と計算のアルゴリズムを考案した．広中平祐も特異点解消問題を考える中で同様の概念に到達している．その後，Mathematica や Maple など代数演算（シンボリック計算）を可能にする計算機ソフトの発達が相俟って現在の隆盛を見るに至っている．

巨大素数が暗号に使えるのは，素数を発見するのが難しく，しかも素数の判定に時間がかかる点にある*1)．素数判定法はいろいろと存在するが，どれも計算機の援用なくしては役に立たない．アメリカでは昔から巨大素数の発見や素因数分解に大きな予算が付いてきた．現在はセキュリティの重要性が高まっているので，暗号理論などはさらに重要性を増している．計算機の性能によるところが大きいが，計算機の性能を調べるのに円周率 π を小数点何桁まで計算できるかを試すという話も聞いたことがある．

筆者の専門は代数幾何学である．Goppa Code を含む代数幾何学符号は，代数曲線上の因子の線形系や代数曲面やもっと高次元の代数多様体の理論を使っているようである．中でも，有限体上定義された楕円曲線の有理点に楕円曲線の群構造を考える楕円曲線符号は，代数多様体が有する群構造を使っている点で，代数学の本質的な応用であるという気がする．代数曲面の中でも，楕円曲面，$K3$ 曲面やエンリケス曲面などは自己同型群が詳細に調べられて複雑な構造をもっているので，符号理論や暗号理論に使われるのではないかと思う．

ミシガン大学のドルガチェフは代数多様体の自己同型群に詳しいが，彼に一度言われたことがある．実は，私の専門はアフィン代数多様体を取り扱うアフィン代数幾何学である．彼によれば，アフィン代数幾何学の結果は複雑で難しい．専門外の人たち，例えば物理学者などには理解しにくい．遠まわしであるが，彼の言いたいことは，単純で興味を喚起する美しい構造が他分野の人たちの理解を得るのに必要であるということである．考えてみると首肯できる点もあるのである．

それでも，アフィン代数幾何学の中心問題の一つである多変数多項式環の自己同型群（とくに，その中の順自己同型写像）を使った暗号をパデュー

*1)　フェルマー数 $2^{2^n}+1$ やメルセンヌ数 2^n-1 を使って巨大素数探しが行われている．インターネットで調べてみると，2013 年の時点で最大の素数はメルセンヌ数 $2^{57,885,161}-1$ で，この素数は 17,425,170 桁とのことである．

大学のモーが提唱している[3]．まだ，実用化には至っていないようであるが．

代数学の応用だけでなく，代数学の新しい発展のためには，深い示唆を与える具体的な例や問題をできるだけ徹底して，しかも種々の観点から調べることが必要のようである．印象深く残っている記事がある[1]．それはインタビューアーのミニオがアティヤに彼の仕事や，そのやり方，または数学の見方について尋ねたもので，アティヤも実に率直に考え方や見方を話している．中でも印象深いのは，数学者は自分で孤立してしまっては駄目であること，大問題を解くという意気込みで研究を始めようとするよりも，興味深い例や興味深い仕事を自分なりに理解しようと努めることで本当に解ける問題に出会うことができるということ，問題を解くアイデアは他分野の人たちとの出会いから偶然に生まれることが述べられている．印象深く記憶に残っているのは，定理を証明することよりも，多くの例に出会ってそれらを取り巻く背景を理解することが新しい結果に結びつくと話している点である．自分の研究を他分野の専門家に理解してもらおうと努力することで，その対象の本質が浮かび上がってくるのではないかと思われる．

筆者が大阪大学に在籍していた当時，ヴィトゲンシュタインの科学哲学を研究していた（故）奥雅博と，数学は自然科学であるか哲学と同列の形而上学であるかということで議論したことがある．奥雅博はヒルベルトの公理主義などを持ち出して，自然現象に基づかないことを研究していると主張したので，筆者が持っている数学に対する感覚と大いに異なるので異論を述べたことから議論が生じたのである．大袈裟に言うと，数学の研究で生じた結果は自然の真理を発見したような感覚を生じるのである．このような感覚を持つ数学者は少なからずいると思うが，数学外の分野では，数学は形而上学と主張する研究者が多いのが実情である．筆者は数学も自然科学の一分野として，他分野の専門家と交わることが大切であると思う．

1990年代であったと思うが，インドのタタ研究所に滞在していたとき，インドとロシアの二国間数学シンポジウムが開催されてアーノルドが参加していた．一夜，タタの教授が開いた少人数のパーティでアーノルドと同席する機会に恵まれて，旧ソ連時代のエリート教育の話を聞いたことがある．要するに，数学の才能に恵まれた若者は数学の中に孤立せずに，積極的に他分野の若者と交流させられたということであった．

最後に，もう一つ思うことがある．ロシアやオランダなどを訪問して出会った数学者が自国の伝統とするような得意な数学分野を大切にし，蓄えた知識のノウハウを機会あるごとに発展させようとしていることである．例えば，ロシアにおける群の表現論やオランダにおける整数論である．「生き字引」のような人がいて，確実な情報と指針が得られるので尊敬を集めている．多分，ヨーロッパの各国で，幾何や解析など様々な分野で同じ事情があるものと思う．新しい数学の潮流に乗り遅れないことは大切であるが，温故知新も大切ではなかろうか．時が幸いして才能豊かな若者が現れたとき，既に得られた知見を革新して新しい発見と応用に結びつけていくことがあるに違いないと考える．

これまでに述べたように，数学を自然科学の一分野ととらえ，他分野との交流を通して具体的な問題を考え，美しい結果と構造を尊重する．また，得られた知見は世代を超えて伝えていく．このような姿勢が代数学（ひいては数学）の本質的な応用につながっていくのではなかろうか．

参考文献

1) M.F. Atiyah and R. Minio, An interview with Michael Atiyah, *The mathematical intelligencer*, March 1984, Vol.**6**, Issue 1, 9–19.
2) 川中宣明，暗号の数理，『現代数理入門』（宮西正宜・茨木俊秀編著）第1章，関西学院大学出版会，2009.
3) T.T. Moh, A public key system with signature and master key functions, *Communications in algebra*, **27**, no.5, 2207–2222, 1999.

（みやにし・まさよし，大阪大学名誉教授）

学習理論と代数学

小林　正典

はじめに

——今日はちょっと整数の数当てをやってみましょう．最初が 2，そして 3，次の数は？

——4？

——残念，5 でした．次の数は？

——素数かな．7？

——残念，8 でした．次の数は？

——階差を取ってみよう．2 から 3 は 1 増えて，3 から 5 は 2 増えて，5 から 8 は 3 増えている．階差が 1, 2, 3 となっているから，次は 4 増やして，12？

——残念，13 でした．次の数は？

——あっ，2, 3, 5, 8, 13 とくれば，フィボナッチ数列に違いない！ $8+13=21$？

——正解！

さて，出題者が順に整数 $a_0, a_1, a_2, \ldots$ を言っていくとき，解答者はいつかは正しく次の数を与えられるようになるものであろうか．もちろん，整数をランダムに与えるのでは，何が正解か不正解か納得できない．そこで，出題者は何か定めた規則（アルゴリズム）に従って次の値を与えていくことにする．上の例では，フィボナッチ数列（の途中から）というのが実は正解なので，規則を見抜いた後はずっと正答を返し続けることができる．

もし「等差数列に限る」という前提で行うなら，簡単である．初項と公差が決まれば数列は決まるので，最初の 2 つの項から一般項が求まる．

等差数列の一般項は項数 n の 1 次式で表されるが，これが 2 次式ならどうであろうか．2 次式は 3 つの係数で決まるので，最初の 3 項で完全に決定できる[*1)]．また，2 項では定まらない．

フィボナッチ数列のようにある 3 項間漸化式 $a_{n+2}=pa_{n+1}+qa_n$（p, q は定数）を満たす，とする場合ならどうであろうか．未知数としては p, q と最初の 2 項 a_0, a_1 の 4 つであるから，最初の 4 項がわかれば一般項 a_n が決定できそうである．確認は読者にお任せする（p, q は必ずしも求める必要がないことに注意）．

何かあるアルゴリズムに則っている問題ならば，いつかは正答に辿り着くのであろうか？ それとも何らかの制約がないと，いつまでたっても正答を与えられないことがあり得るだろうか？

データが与えられたときにそこから規則を見出すことは，近年ではデータマイニングなど機械学習の大きな研究対象になっている．学習理論と一口に言っても広く，例えば統計を基礎とした学習理論もあるし，代数幾何を学習理論に応用した渡辺澄夫氏らの研究[7)]も有名である．本稿では，特に，筆者が関わった計算論的学習理論の話題を採り上げて，そこに代数学が用いられている様子を説明したい．

*1) 一般に異なる $d+1$ 点での値から d 次多項式が一意的に定まり，ラグランジュ（Lagrange）の多項式近似で具体的に与えられる．また，任意の（非負）整数に対し整数を与える多項式は，ジョルダン（Jordan）の階乗関数の整数係数 1 次結合で表される．

1. 計算論

まず，計算論的学習理論で用いられる計算論の基礎的な事項について解説しよう．詳細は例えば文献 2, 3) を参照していただきたい．

1.1 言語

文字の有限集合（**アルファベット**）を Σ とする．文字を 0 個以上並べたものを**語**（文脈によっては**文**）といい，語の全体を Σ^* で表す（* の意味は後述）．$\Sigma = \{$ い，や $\}$ のとき，Σ^* には「いい」「いや」「やや」「いやいや」といった語が入る．

Σ^* には**連結**（ならべて 1 つにすること）という演算が定まる．「いや」と「いい」の連結は「いやいい」である．結合法則を満たし単位元は**空列**（文字 0 個の列）である．Σ^* は**モノイド**である．

Σ^* の中には，意味をなすと定める文字列もあれば，ナンセンスなものもある．前者がはっきり定まっている場合を想定して，Σ^* の部分集合 L を**言語**と呼ぶ．

1.2 言語族

アルファベット Σ は n 文字からなるとしよう．言語 L はどのくらいあるであろうか？

l 文字からなる語は直積 Σ^l の元であるから n^l 個ある．語の全体 Σ^* の濃度は $1+n+n^2+n^3+\cdots$ つまり可算無限 $\aleph_0$ である．それぞれの語について L に属するかどうか決めることで，L が定まる．よって，言語全体の集合の濃度は $2^{\aleph_0}$ すなわち実数の濃度と同じである．どの言語であるかを指定しようとしても，有限のデータではラベル付けしきれないほど多い．すべての実数を表記するのに有限小数展開では足りないようなものである．

言語の中にも，重要なものとそうでないものがあるであろうから，言語の扱いやすい集まりを指定することにする．（共通のアルファベットをもつ）言語の集合を**言語族**という．ただし，使用するアルファベットが異なる言語がいろいろあっても，すべての文字を例えば 2 進数でコード化できれば，共通のアルファベットをもつ言語として扱える．

1.3 正則言語

基本的な言語族として，「正則表現」で表すことのできる言語の集合を考えよう．正則表現はアルファベット Σ に数個の記号を加えて作られる．

例えば Σ を英字の集合としよう．ab という表現で，集合 $\{\mathrm{ab}\}$ を表す．$\mathrm{ab} \cup \mathrm{ba}$ は，和集合 $\{\mathrm{ab}\} \cup \{\mathrm{ba}\}$ すなわち $\{\mathrm{ab}, \mathrm{ba}\}$ を表す．

$\mathrm{ab^*c}$ で，ac, abc, abbc, abbbc, ... といった，a で始まり，0 個以上の b を並べ，c で終わる語の集合を表す．* は**クリーネ**（Kleene）**のスター**と呼ばれ，直前の文字列を 0 個以上繰り返したものを表す．$\mathrm{a(ba)^*}$ は，abababa のように，a と b が交互に現れ最初と最後は a となる語の集合を表す．ura(niwa)*torigairu が表す集合には ura-torigairu（裏取りが要る）も，uraniwatorigairu（裏には鳥がいる）も，uraniwaniwaniwaniwani-waniwaniwatorigairu（裏庭には二羽，庭には二羽，鶏がいる）も属する．もちろん他の無意味な文も入っている．

上のように，Σ の元（および空列）に，連結・和集合・クリーネのスターという 3 種の演算を有限回施して得られる文字列を**正則表現**という．演算の優先順位を表すために括弧は適宜用いてよい．正則表現で表される Σ^* の部分集合を**正則言語**という．

正則言語 L と語 $\mathrm{w} \in \Sigma^*$ を与えたとき，w が L に属するかどうかを判定できるであろうか．

1.4 有限オートマトン

双六（すごろく）では，「振り出し」から出発して，サイコロの目によってマス目にコマを進めながら「上がり」を目指す．マス目によっては「振り出しに戻る」などという「残念」なものもあるかもしれない．

一般に，有限個のマス目があって，振り出しと上がりのマス目が指定されており，それぞれのマス目では次のサイコロの出目に応じて（あるいは自動的に）進むマス目が決まっているとする．この双六は**有限オートマトン**，正確にはその**状態遷移図**と呼ばれる．

サイコロの目の有限集合を Σ とするとき，振り出し（初期状態）から上がり（終了状態）に到達する出目の列を，この有限オートマトンが**受理**する語といい，その全体を受理する言語という．

なお，上では双六とさいころの目の例えを用いたが，出目の列をさいころを振ってランダムに与える必要があるわけではないし，$\Sigma = \{1, 2, \ldots, 6\}$ である必要もない．

次が成り立つ．

定理 1.1 正則言語はある有限オートマトンで受理される．逆に，有限オートマトンで受理される言語は正則言語である．

1.5 正則でない言語

$\Sigma \neq \varnothing$ を固定したとき，正則言語は有限個の文字からなる有限列で表されるから，高々可算個しかない．言語は非可算個あるから，正則でない言語が存在する．例を挙げるために次を用いる．

定理 1.2（ポンピング補題） L を正則言語とすると，次の性質を満たす $l \in \boldsymbol{N}$ が存在する：
（性質） 長さ l 以上の任意の語 $\mathrm{w} \in L$ に対し，$\mathrm{w} = \mathrm{xyz}$ となる $\mathrm{x}, \mathrm{y}, \mathrm{z} \in \Sigma^*$ が存在し，y は空列でなく，xy の長さは l 以下で，任意の $n \in \boldsymbol{N}$ に対し $\mathrm{xy}^n\mathrm{z}$ は L に属する．

よって，十分長い L の語については，その一部を繰り返し並べて L の語が作れる．

証明のアイデアを説明しておく．双六では現在のコマの位置が変化するだけなので，マス目の個数だけしか状態がない．したがって，入力文字数が大きくなると受理されるまでにどこかで同じマス目を 2 回通ることがある．そのループの間の出目の列が y である．

さて，$L = \{\mathrm{a}^n\mathrm{b}^n \mid n \in \boldsymbol{N}\}$ で，a が 0 個以上並びさらに b が同数だけ並ぶ語の全体を表す．$\mathrm{aabb} \in L$ であるが，$\mathrm{abab}, \mathrm{abb} \notin L$ である．

L は有限オートマトンでは受理できないことが示せる．実際，もし表されるとすると，ポンピング補題より，十分大きな $n \in \boldsymbol{N}$ に対し，ある $\mathrm{x}, \mathrm{y}, \mathrm{z} \in \Sigma^*$ が存在して，$\mathrm{a}^n\mathrm{b}^n = \mathrm{xyz}$ と書けるはずである．$\mathrm{xy}^2\mathrm{z}$ が L に属さないことは容易に確かめられる．矛盾．

1.6 計算可能

現代の計算機はもちろん双六よりずっと強力である．その理論的モデルとなったのが，チューリング（Turing）により，人間が黒板に文字を書いたり消したりして計算することを模して考えられた**チューリング機械**である．チューリング機械は，双六にあたる状態遷移図，外部入出力装置であるテープヘッド，記憶媒体であるテープ（直線状でマス目をもつ）からなる．

入力データは予めテープに書き込んである．テープヘッドが指すマス目の文字を入力として受け取り，状態遷移図の指示に従って，必要ならテープに文字を書き込んだり，テープヘッドを左右に 1 マス移動させたり，双六のマス目を移動したりする．

入力を与えたとき，有限ステップ内に終了状態に到達して，そのときのテープの内容が正しい出力となる関数を**計算可能**な関数であるという．これが通常の意味で，アルゴリズムで計算できるという最も広い概念を与えているのである．

言語 L は，ある計算可能関数の定義域（あるチューリング機械が受理する語の全体）となるとき**チューリング可算**であるという．さらに補集合もチューリング可算であるとき（つまり任意の語 w に対し $\mathrm{w} \in L$ であるかないか判定できるとき）**計算可能**であるという．

例えば，L として，正の整数 a, b, c で $a^n + b^n = c^n$ を満たすものが存在するような 3 以上の整数 n（の十進表記）の集合を考える．与えられた n に対し，正の整数のすべての組 (a, b, c) について 1 つずつ条件を満たすかどうか順次確かめていくプログラムは容易に書ける．よって L はチューリング可算である．しかし，計算可能であること（$L = \varnothing$ である！）は，長い間未解決問題であった．

1.7 忙しいビーバーの問題

関数に対して，存在することと，計算可能であることは異なる．計算は，具体的な手続きを構成して答えを与える．存在することが示されたとしても，その証明に選択公理を用いていたり，存在しないと仮定して矛盾を導くという背理法を用いたものであると，証明から手続きを構成することができないのである．

関数として存在しても，あまりに急に増加する

ため計算可能でない例として，ラドー（Radó）の「忙しいビーバーの問題」*2) がある．入力列はなく，テープで読み書きできる文字は空白の他は1種類のみとするチューリング機械を考える．有限オートマトンでない最も単純なチューリング機械といえよう．内部状態（マス目）の数を n とするとき，停止したときに最大何個の文字をテープに書き込んでいることができるか，というのが問題である．

これが存外に多いのである．答えを $\Sigma(n)$ と書くとき（アルファベットの Σ とは無関係），$n=1,2,3,4$ に対して $1,4,6,13$ となることはわかっているが，$n\geq 5$ では未解決である．$n=5$ の記録保持者の一人である Heiner Marxen 氏のホームページによると，現在の記録は $\Sigma(5)\geq 4098$，$\Sigma(6)>3.514\times 10^{18276}$ だそうである．

$\Sigma(n)$ は，n の関数として計算可能でないことがラドーによって示されている．n を1つ決めるとチューリング機械は有限個しかない．そこで，それらを総当りで構成して出力される文字数を比較しようとしたとする．ところが，一つ一つがいつか停止するかどうか，わからないのである．$n=5$ の場合，いくつかのプログラムが今でも動き続けているという噂である．

2. 有限性と代数

いつかは終わるが，それがいつかは必ずしもわからない．代数系においては，ネーター（Noether）性に見られる性質である．

2.1 モノイドイデアル

整数全体の集合 $\boldsymbol{Z}$ は足し算に関して可換群になる．つまり，任意の2元の和が定まり，交換法則と結合法則を満たし，単位元0が存在し，n に対して逆元 $-n$ がある．

自然数全体の集合 $\boldsymbol{N}$ にも足し算が定まっている．しかし引き算はできるとは限らず，$2-3$ のように負になることがある．本稿では $\boldsymbol{N}$ は0を

*2) 命名は，テープヘッドが左右にせっせと動き続けるさまを，ダムを作る「ビーバーのように忙しい」(busy as a beaver) という英語の成句にひっかけたものであろう．

含む流儀を採用しているので，$\boldsymbol{N}$ は単位元を含む可換半群，すなわち，**可換モノイド**である．

多項式環のべき指数の全体が可換モノイドをなすことを念頭においており，環の積がモノイドの和に対応する．

可換モノイド S の部分集合 I が（モノイド）**イデアル**であるとは，

$$a \in I,\ s \in S \Rightarrow a + s \in I$$

を満たすことをいう．イデアルは S の部分半群でもある．次は定義から直ちに従う（定義もそうであるが，可換環の場合と微妙に異なる）．

定理 2.1　$\varnothing$ はイデアルである．イデアルの任意個の交わりや和集合はイデアルである．

$a \in S$ に対し，$(a) = \{a + s \mid s \in S\}$ は a を含むイデアルである．(a) を a で**生成**されたイデアルという．$S = (0)$ である．一般に S の部分集合 A に対し，$(A) = \{a + s \mid a \in A,\ s \in S\}$ を A で生成されたイデアルという．A を含む任意のイデアルは (A) の元をすべて含むので，(A) は A を含むイデアルで，包含関係に関して最小のものである．任意のイデアル I は I 自身で生成されるが，ある有限集合 A によって $I = (A)$ と書けるとき，**有限生成**であるという．

2.2 ネーター性

可換モノイド S がネーター性を満たすとは，次の同値な性質を満たすことである．

(1)（極大条件） イデアルからなる空でない任意の集合 $\mathscr{I}$ は，包含関係に関する極大元をもつ．

ただし，$I \in \mathscr{I}$ が $\mathscr{I}$ の極大元であるとは，I より真に大きな元が $\mathscr{I}$ 内にないことである．

(2)（有限条件） 任意のイデアルは有限生成である．

(3)（昇鎖条件） イデアルの任意の昇鎖 $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ に対し，ある $n \in \boldsymbol{N}$ が存在して $I_n = I_{n+1} = \cdots$ となる．

同値性の証明は可換環の場合と同様であり，$(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (1)$ の順に示せる．$(3) \Rightarrow (1)$ の部分では選択公理を用いる．ただしイデアルの和を使うところは和集合である．

2.3 ディクソン性

順序集合 S が**ディクソン**（Dickson）**性**をもつとは，次の同値な条件を満たすことである．

(D1) S の任意の部分集合 A に対し，A のある有限部分集合 B で，$\forall a \in A, \exists b \in B, b \leq a$ が成り立つ．

(D2) 無限列 $a_0, a_1, a_2, \ldots \in S$ に対し，無限部分列 $a_{i_0} \leq a_{i_1} \leq \cdots$ $(i_0 \leq i_1 \leq \cdots)$ が取れる．

(D3) 無限列 $a_0, a_1, a_2, \ldots \in S$ に対し，$i < j$ かつ $a_i \leq a_j$ となる $i, j \in \boldsymbol{N}$ が存在する．

順序集合 S, T の直積 $S \times T$ に順序を「$(a,b) \leq (a',b') \iff a \leq a'$ かつ $b \leq b'$」で定める．

定理 2.2　S, T がディクソン性をもてば，$S \times T$ はディクソン性をもつ．

$\boldsymbol{N}$ は明らかにディクソン性をもつから次が従う．

定理 2.3（ディクソンの補題）　$\boldsymbol{N}^n$ はディクソン性をもつ．

$\boldsymbol{N}^n$ では $b \leq a \iff a \in (b)$ であるから，次が従う．

定理 2.4　$\boldsymbol{N}^n$ の任意のモノイドイデアルは有限生成である．

体上の n 変数多項式環では，べきの全体が $\boldsymbol{N}^n$ であり，上を用いて次が示せる．

定理 2.5（ヒルベルト（Hilbert）の基底定理） 体上の多項式環はネーター環である．

具体的にグレブナ（Gröbner）基底というイデアルの生成系をブッフベルガー（Buchberger）のアルゴリズムで計算可能である．文献 1) を参照．

歴史的にはヒルベルトの基底定理が先に証明されている．証明はネーター性に基づく非構成的なもので，これに対し不変式論の大家であるゴルダン（Gordan）が，「これは数学ではない．神学である.」と言ったという有名な伝説がある．

3. 計算論的学習理論への応用

3.1 正データ極限同定可能

チューリング可算な言語の族 $\mathscr{C}$ が与えられて

おり，$\mathscr{C}$ に属する言語 L が秘かに選ばれているとする．教師は L に属する語を 1 つずつもれなく，$w_0, w_1, \ldots$ と与えていく（**枚挙**するという）．これを**正提示**という．「語 w は L にはありません」というのは**負提示**というが，本稿では用いない．語が 1 つ提示されるたびに生徒は L を推測し，$\mathscr{C}$ の元 $L_0, L_1, \ldots$ を与えていく．なお，本節の定式化では L は集合であり数列ではないので，冒頭の数当てのように枚挙する順番が決まっているわけではない．

生徒が正解 L を与えても，教師は「それが正解です」とは言わないものとする．しかし，ある時点で正しい推測 L にたどり着けば，その後も L に含まれる語がずっと提示されるので，以後は生徒は推測を変える必要はない．このとき，生徒は自分が正解を導き出したことは知らないのだが，正答を学習したとみなすのが極限学習の考え方である．

念頭にあるのは，例えば人工知能による未修言語の習得である．話されている言語の実例を聞いて，正しい文を作るルールを身につけようとする．試行錯誤の末，ついに正しい言葉を話せるようになったとしても，教える側はルールを明文化して作文しているわけではないので，そのルールで完璧ですとは言えない．でも使う言葉に齟齬はないであろうし，それまでのルールで理解できない言い回しに出会えばそのときまた直すのである．

もし，どの L に対してもいつかは正しい推測を与えることができるとき，すなわち，任意の L とその正提示に対し，ある $n \in \boldsymbol{N}$ が存在して，$L = L_n = L_{n+1} = \cdots$ となるアルゴリズムが存在するとき，$\mathscr{C}$ は**正データ極限同定可能**であるという．

ゴールド（Gold）によると，すべての有限部分集合と少なくとも一つの無限集合を含む言語族，よって例えば正則言語族ですら，正データ極限同定可能ではない．

3.2 判定条件

言語族が正データ極限同定可能であるための必要十分条件が Dana Angluin によって与えられている．まずいくつか言葉の準備をしよう．

$L \in \mathscr{C}$ とし，T を L の有限部分集合とする．T が L の**有限証拠集合**であるとは，$L' \in \mathscr{C}$ が T を含めば L' は L の真部分集合ではないことをいう．また，T が L の**特徴例集合**であるとは，T を含む $L' \in \mathscr{C}$ は L を含むことをいう．よって，特徴例集合は有限証拠集合である．

次の条件を考える．

(EC1) 任意の $L \in \mathscr{C}$ に対し，有限証拠集合を枚挙する手続きが存在する．

定理 3.1（Angluin） $\mathscr{C}$ が正データ極限同定可能 $\Longleftrightarrow$ $\mathscr{C}$ が (EC1) を満たす．

その他に言語族 $\mathscr{C}$ に対する様々な条件を列挙する．

(C1) 任意の $L \in \mathscr{C}$ が有限証拠集合をもつ．

(C1) は (EC1) と同値でなく，正データ極限同定可能とは限らないことが知られている．

(C2) 任意の $L \in \mathscr{C}$ が特徴例集合をもつ．

(C3) 任意の語の無限列 $w_0, w_1, \ldots$ に対し，言語の無限列 $L_0, L_1, \ldots$ で，すべての $n \in \boldsymbol{N}$ に対し $\{w_0, w_1, \ldots, w_{n-1}\} \subset L_n$ かつ $w_n \notin L_n$ となるものは存在しない（**有限の弾力性**）．

(C3) が満たされるなら，正答を言い当てられたとき，それまでの正提示に矛盾が出ないように正解をそこでこっそり変えて言い逃れ続ける，なんてことはできない．

(C4) 各語 w に対し，$w \in L$ となる $L \in \mathscr{C}$ は有限個である（**有限の厚さ**）．

これらの条件の間には次のような関係がある[4]．

$$
\begin{array}{ccccccc}
\text{(C4)} & \Longrightarrow & \text{(C3)} & \Longrightarrow & \text{(C2)} & \Longrightarrow & \text{(C1)} \\
 & & & & \Downarrow & & \\
 & & & & \text{(EC1)} & &
\end{array}
$$

特徴例集合はいかにも代数系の生成系を思い起こさせる．実際，可換環のイデアル全体をモデルとすると，次のように，可換環を学習理論を用いて特徴付ける結果が得られている（文献 5, 6)）．

定理 3.2 $\mathscr{C}$ を可算な可換環 R のイデアル全体からなる族とするとき，次が成り立つ．

$\mathscr{C}$ が正データから極限同定可能 $\iff$ $\mathscr{C}$ が (C3) を満たす $\iff$ R がネーター環.

定理 3.3 可算な素元分解整域 R に対し, $\mathscr{I}$ を R のイデアルの有限個の和集合の全体とする. このとき, $\mathscr{I}$ が正データ極限同定可能 $\iff$ R が単項イデアル整域, となる.

可換環のイデアルの和集合とは何とも奇妙であるが, 代わりに可換モノイドで考えればイデアルの和とは和集合のことなので, 自然な対象になる.

おわりに

同僚の徳永浩雄氏が, 京都大学の山本章博氏と行っていた共同研究に筆者を引き入れてくれたことがこの話の発端であり, 両氏に感謝する. より詳細な内容は文献 4, 6) をご覧いただきたい.

参考文献

1) David Cox, John Little, Donal O'Shea, *Ideals, Varieties, and Algorithms (3rd Edition)*, Springer, 2007;（第 2 版邦訳）D. コックス, J. リトル, D. オシー（落合啓之, 示野信一, 西山享, 室政和, 山本敦子訳）『グレブナ基底と代数多様体入門（上）・（下）』, シュプリンガー・ジャパン, 2000, 丸善出版, 2012.

2) John E. Hopcroft, Rajeev Motwani, Jeffrey D. Ullman, *Introduction to Automata Theory, Languages, and Computation (3rd Edition)*, Prentice Hall, 2006;（第 2 版邦訳）J. ホップクロフト, R. モトワニ, J. ウルマン（野崎昭弘, 町田元, 高橋正子, 山崎秀記訳), 『オートマトン　言語理論　計算論 I, II』, サイエンス社, 2003.

3) Michael Sipser, *Introduction to the Theory of Computation, 3rd Edition*, Cengage Learning, 2012;（第 2 版邦訳）—（太田和夫, 田中圭介, 阿部正幸, 植田広樹, 藤岡淳, 渡辺治訳), 『計算理論の基礎　原著第 2 版　1, 2, 3』, 共立出版, 2008.

4) 榊原康文, 小林聡, 横森貴, 『計算論的学習』, 情報数理シリーズ B-6, 培風館, 2001.

5) F. Stephan and Y. Ventsov, Learning algebraic structures from text, *Theoretical Computer Science*, **268** (2001), 221–273.

6) 徳永浩雄, 山本章博, 小林正典, 「人工知能における計算論的学習理論と Noether 環」, 数学 **59** (2007), 岩波書店.

7) 渡辺澄夫, 『代数幾何と学習理論』, 知能情報科学シリーズ, 森北出版, 2006.

（こばやし・まさのり, 首都大学東京大学院理工学研究科）

計算機科学と代数学

プログラム意味論と普遍代数学

蓮尾　一郎

■　1. 計算機科学とは？　意味論とは？　■

代数学のさまざまな応用についての本特集において，本稿は**計算機科学**――そのうちとくに**意味論**――とよばれる分野に現れる代数学的構造と，その応用について紹介したい．多くの読者のもともとの興味は数学や，多少外れたとしても物理学などだろうから，まず，計算機科学（のうち意味論）とは何をめざす学問なのかを説明していく．

ところでいきなり余談から始める．自分と異なる研究分野の人と話をする際，まず最初にやるべきことは，相手が「何がやりたいのか，何をカッコいいと思うのか」をお互いに理解することである．しかし，そのような目的意識・美意識は本人にとってはすでに刷り込まれた当たり前のことであり，当たり前のことを言葉にして説明するのはとてもむずかしい．この場合の有効な手段は，インフォーマルに徹してともかく「気持ち」をたくさん話すことである．というのはプリンストン高等研究所の学際研究担当教授 Piet Hut さんの受け売りであり，彼は「IZAKAYA に行くといいね」と言うが本稿ではそうもいかない．何が言いたいのかというと，本稿が以下ややくだけ過ぎ感があることの言い訳である．

計算機科学と一口に言っても研究内容はアーキテクチャ，アルゴリズム，ハイパフォーマンス・コンピューティング，ユーザ・インタフェイスなどさまざまであるが，本稿で注目するのは

- 計算機――特にプログラム――の動作，ふるまいを数学のコトバでモデリングして，その本質の理解をめざす**意味論**（semantics）というトピックと，
- その応用，特に計算機システムの正しさを数学的に証明する**形式検証**（formal verification）への応用[*1)]

である．

上の二つの●において「計算機」を「自然界」にとり替えると，そのまま物理学の説明として読めそうなことに注意されたい．実際，我々意味論の研究者が日々行っていることは，たとえば惑星の運動を微分方程式で記述するかのような**数理モデリング**である．ただしもちろん，対象の違いはモデリング手法の違いとして現れる：連続的な自然現象のモデリングには主に解析学的手法によるが，プログラムのそれには代数学的手法を用いるのである．

本稿ではプロセス代数という単純なプログラミング言語を例に，計算機科学における意味論の現場をかいま見てもらうことを目的にする．はじめに注意しておくと，数値計算によるシミュレーションなどの**計算科学**や，数式処理を計算機上で行う**計算機代数**などは本稿のテーマとは別の話である．期待された読者の方には申し訳ない．

■　2. 計算機科学における「有限 vs. 無限」　■

もう少しインフォーマルな話を続けたい．問題は

- 計算機やプログラムのどのような特性ゆえに，代数学的手法が有効なのか？

というものであり，筆者の解答は

- 有限と無限のせめぎあい

である．この点を説明していく．

計算機の行う「計算」とは，足し算や掛け算と言うより「なんらかの手順に従った機械的な作業」と思ったほうが適切だ．このことは，計算機が生活のあらゆる場面において使われる現代においては明らかだろう．

---

*1)「形式」とはおおむね「数学的」の意味．

この手順を記述するのが**プログラム**と呼ばれる有限長の文字列であり，計算機はプログラムにしたがって動作し作業を行う．

本稿のテーマである「意味論」という言葉は，たとえば「自然言語の意味論」というようにも用いられる一般的な言葉だが，本稿の文脈では「プログラムの意味について数学的に考えよう」という意味である．ここで：次のプログラムの意味とはなんだろうか？

```
int add (int x, int y) {
  return x + y;                          (1)
}
```

「足し算だよね」と思った読者はすでに（単純化・抽象化を伴う）数理モデリングを行っており，すなわち意味論の実践者であると言えよう．というのは，多くの実装において `int`（整数）型は 32 ビットのデータ型であり，足し算の結果が桁あふれするかもしれないのである．このように数理モデリングによって失われるディテールが存在する一方で，単純化された「意味」を用いてプログラムの性質を数学的に記述できるのは大きな利点である．このあたりの事情は，（大きさを持たない質点が登場したりする）物理学などでも同じであろう．

プログラムの意味について考えると，本節はじめの「有限 vs. 無限」の対比が直ちに現れる．次のプログラムを考えよう．

```
infinite (int x) {
  print x;
  infinite (x + 1 mod 2);                (2)
};
infinite (0);
```

関数 `infinite` は自分自身の**再帰呼び出し**を行うため，このプログラムを実行すると画面上に

```
0,1,0,1,...
```

と表示され続けるはずである．ここで重要なのは，計算機が動作し続けることにより**有限長**のプログラムが**無限長**の意味を生成することである．

ここで，大学 2 年くらいで習う（素朴）集合論で考えてみると，

- プログラムは文字の有限列．すなわち，文字の集合（アルファベットとよばれ，ふつう有限集合）を Σ とすると，プログラムは $\Sigma^* = \bigcup_{n\geq 0} \Sigma^n$ の元．
- プログラムの意味（またはふるまい）は何らかの集合 Γ の元の無限列，すなわち $\Gamma^{\mathbb{N}}$ の元．

濃度を比較すると $|\Sigma^*| = \aleph_0 < \aleph_1 \leq |\Gamma^{\mathbb{N}}|$（ただし $|\Gamma| \geq 2$ とした）．この帰結として，

- 可能なふるまい全体のうち，あるプログラミング言語を用いて表現できるものはごくわずか

であることがわかる[*2]．

計算機科学の本質はまさにこの点にある：つまり，**無限長のふるまいについて，有限長のプログラムを用いて記述し，考える**のである．たとえば，

> `infinite` を用いた上のプログラム (2) のふるまいに `0` が無限回現れるかどうか？

という問題を考えよう．これを調べるために，ふるまいとしての無限列 0, 1, 0, 1, ... を直接調べるわけにはいかない——無限列を尽くす前に我々の有限の寿命が先に尽きてしまう．しかしもともとのプログラム（すなわち無限列の有限的表現）からスタートして，その構造を使ってやれば，余帰納法（coinduction）という手法を用いた証明がものの数行で書けてしまう．

3. 代数学とは——普遍代数学

有限長のプログラムのもつ無限長のふるまいについて説明してきた．ここでなぜ代数学が登場するのだろうか？

そもそも「代数学」という言葉が何を指すのかについて，読者のみなさんもそれぞれイメージをお持ちのことと思うし，本特集では代数学のさまざまな側面が紹介され応用されている．ここでは一つ大胆なスローガンをぶちあげてみよう．

> 代数学とは**構文と意味の分離**とみつけたり

この見方を説明するため，さまざまな種類の代数系を統一的に扱う**普遍代数学**（universal algebra）のほんのさわりを導入する．普遍代数学は歴史的には**論理学**の一分野であり，意味論で用いる「代数学」とは多くの場合普遍代数学を指す．

定義 1 ● **代数シグニチャ**（signature）とは，集合の

*2) プログラムで記述できるふるまいはある意味で**有理的**（rational）であると言える．ただしこれは循環的とは違う：無限列 0, 1, 0, 0, 1, 0, 0, 0, 1, ... は（際限なく大きなメモリを仮定すれば）再帰プログラムで生成できる．

無限列 $\Sigma = (\Sigma_0, \Sigma_1, \Sigma_2, \dots)$ のこと．各 $n \in \mathbb{Z}_{\geq 0}$ に対し，元 $\sigma \in \Sigma_n$ を n **項演算子**とよぶ．

- 代数シグニチャ Σ に対し，次のルールを有限回適用して得られる記号列を Σ **項**とよぶ．
  - ◦ **変数** $\mathtt{x}, \mathtt{y}, \ldots \in \mathbf{Var}$ は Σ 項．
  - ◦ $\sigma \in \Sigma_n$ が n 項演算子で，$t_1, \ldots, t_n$ がそれぞれ Σ 項ならば，$\sigma(t_1, \ldots, t_n)$ は Σ 項．

  ただし変数の可算無限集合 $\mathbf{Var}$ を別に定めておくものとする．
- Σ 上の**等式公理**とは，Σ 項のペア (s,t) のことをいう．等式公理 (s,t) を $s = t$ とも書く．

例を挙げると，

$$\Sigma_{\mathrm{gp}} = \bigl(\{\mathtt{e}\}, \{\mathtt{i}\}, \{\mathtt{m}\}, \emptyset, \emptyset, \ldots\bigr)$$

は代数シグニチャであり，

`m(e(),x) = x` や `m(i(x),x) = e()`

は Σ_{gp} 上の等式公理である．

上の定義によると，Σ 項を作るためには変数 $\mathtt{x}, \mathtt{y}, \ldots$ あるいは 0 項演算子を使った $\sigma()$ から始めて，これらを $n (\geq 1)$ 項演算子を使って順次組み合わせていくことになる．こうしてできる Σ 項は常に有限長の文字列であることに注意しておく．

上の例からは「群のことかなあ」という雰囲気が伝わってくるが，ポイントは**記号の意味をまだ考えないこと**である．すなわち，演算子 `m` にはまだ何の意味も定義されていないし，括弧 `(` や `)` もただの記号であり，さらには，記号 `=` はただの区切りの役割しか果たしていない．次の定義ではじめて意味が登場する．

定義 2
- **代数仕様** (algebraic specification) とは，代数シグニチャ Σ と，Σ 上の等式公理の（任意の）集合 E のペア (Σ, E) のこと．
- (Σ, E) **代数**とは $\bigl(X, (\llbracket\sigma\rrbracket)_{\sigma \in \Sigma}\bigr)$，ただし
  - ◦ X は空でない集合（**台集合**），
  - ◦ 各 n と各演算子 $\sigma \in \Sigma_n$ に対して，$\llbracket\sigma\rrbracket$ は $X^n \to X$ の型の関数（**演算子 σ の解釈**）

  であり，E に属する等式公理すべてを「満たす」もののことをいう[*3]．

つまり，群を例にとって考えると，

- 群の定義はある代数仕様 $(\Sigma_{\mathrm{gp}}, E_{\mathrm{gp}})$ によって与えられ，
- 具体的な群（対象群，一般線形群，…）はそれぞれ一つの $(\Sigma_{\mathrm{gp}}, E_{\mathrm{gp}})$ 代数を与える，

というわけである[*4]．

以上の定義はまだるっこしいかもしれない．しかしここで行ったのは**計算機科学（と論理学）の基礎の基礎**[*5]，すなわち，記号列を取り扱う**構文論** (syntax) と，記号列の意味を数学的に定義する**意味論** (semantics) との分離である．ここで用いた記号 $\llbracket - \rrbracket$ は，論理学・計算機科学において一般に「文字列の意味」を表すために用いられる．

以上では群や環などの代数的概念が本質的に構文論的であることをみてきた．このことは代数学的手法の一類型，すなわち**数式変形**の基礎をなす：(Σ, E) 代数の元を Σ 項を用いて書き表したのち，E に属する等式公理を用いて変形していくのである．代数学での構文論の重要性の例は他にも，自由群や加群のテンソル積の構成——記号列の同値類を用いて記述される——に現れる．また，最近数学の多くの分野で用いられる**オペラド** (operad) の理論は，上記の普遍代数学の「いとこ」のような存在である．

話を戻して：計算機科学と代数学の関わりについてはすでに明らかであろう．すなわち，双方とも

有限長の記号列による表現を基礎としている

のである（前者においてはプログラム，後者においては数式つまり Σ 項）．

ところで，計算機科学と代数学の関わりをしめす余談としては次のようなものもある．そもそも英語の algebra という単語の語源はアラビア語の al jebr（ばらばらにしたものを組み合わせる）であり，その単語を最初に著書のタイトルに使ったのが 9 世紀のイスラム科学者 al-Khwārizmī であり，彼の名前がアルゴリズム algorithm の語源となった．

---

*3) 「満たす」の定義の概略を述べる．変数から X の元への割り当て（**付値**）$J\colon \mathbf{Var} \to X$ を定めると，項 t の**解釈** $\llbracket t\rrbracket_J \in X$ が帰納的に（小さな項から順々に）定義できる．等式公理 $s = t$ が**満たされる**とは，すべての付値 J に対して $\llbracket s\rrbracket_J = \llbracket t\rrbracket_J$ となることをいう．最後の $=$ はただの区切り記号 `=` でなく，X の元としての等しさであることに注意．

*4) 正確には，「群の定義の一表現」が代数仕様 $(\Sigma_{\mathrm{gp}}, E_{\mathrm{gp}})$ に相当すると言うべきである：たとえば，適切に等式公理を選ぶことによって，2 項演算 $(-_1)^{-1} \cdot (-_2)$ のみを用いた表現も可能．

*5) そもそも計算機（Turing 機械）は 20 世紀初頭の論理学の隆盛の中から現れた．

4. プロセス代数

本稿の残りでは Plotkin によるプロセス代数の構造的操作意味論を通して，「意味論の働く現場」を見てもらいたい．

並列システム論（concurrency theory）という分野がある．マルチコア・プロセッサからインターネットまで，計算機を並列実行するのは現在の流行である一方，並列システムのふるまいについて考えるのはとてもむずかしい——おおざっぱに言って，計算ユニット数の増加に対してシステム全体の複雑さは指数関数的に増加する．**プロセス代数**（process algebra）とは，並列システム論においてシステムを表現するのに用いられる単純な「プログラミング言語」の一群を指す．

多くのプロセス代数は定義 2 のような単純な代数シグニチャと同一視できる（ゆえにプロセス「代数」）[*6]．次の代数シグニチャを考えよう．

$$\Sigma_{\mathrm{pa}} = \bigl(\{\mathsf{a},\mathsf{b},\mathsf{c},\mathbf{0}\}, \{!\}, \{\,\|, +\}, \emptyset, \emptyset, \ldots\bigr).$$

これらの演算子の意味を正確に定義することがそもそもの問題なのであり，そのやり方を後で説明するのであるが，とりあえず「気持ち」を述べておこう．Σ_{pa} 項のそれぞれは並列システムを表す**プログラム**であり，

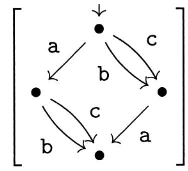
- $\mathsf{a},\mathsf{b},\mathsf{c}$ は（**原子**）**アクション**．便宜的に，「画面に a（または b, c）を出力」と考えよう．
- $\mathbf{0}$ は**停止**を表す．
- $s \parallel t$ はシステム s,t の**並列実行**を表す．
- $s + t$ はシステム s,t の**非決定和**（どちらかを任意に選んで実行するが，選ばなれなかった片方については忘れてしまう）．
- $!s$ は s の**複製**（s のコピーを可算無限個作って，これらを並列に実行する）．

例として Σ_{pa} 項 $\mathsf{a} \parallel (\mathsf{b}+\mathsf{c})$ を考えると，その表すシステムは

- システム a と b+c が並列実行しており，どちらが先にアクションを行うかわからない．前者が先の場合は a を表示し，後者が先の場合は b と c のどちらかが表示される（そしてもう片方については忘れてしまう）．
- 次に，上で a が表示された場合は，残りの b + c がアクションを行う．逆も同様．

*6) 一般にプログラミング言語を代数的に表現するには，**多種シグニチャ**（many-sorted signature）が必要である．

このように，並列システムのふるまい——すなわちプロセス代数のプログラムの意味——を考えると，並列実行の**競合**（race）による非決定性が不可避的に現れる．これを数学的に記述するためには，プログラム (1) の場合のように入力値から出力値への関数と考えたり，プログラム (2) の場合のように画面出力の無限列とするのではうまくいかない．そこで並列システム論では以下のような**ラベル付き遷移系**（labeled transition system）を用いることが多い．

$[\![\mathsf{a} \parallel (\mathsf{b}+\mathsf{c})]\!] =$  .　　(3)

つまり，一番上の状態 • から始まって，アクション $\mathsf{a},\mathsf{b},\mathsf{c}$ を行いながら状態を遷移していくわけである．この遷移系は上記の「気持ち」を数学的に表現しており，このようにシステム実行を追いかけるスタイルの意味論を**操作意味論**（operational semantics）と呼ぶ．

さて問題は，上記 (3) のような操作意味論をどのようにして数学的に正確に定義するかであり，一つの答えが Plotkin の**構造的操作意味論**（structural operational semantics, SOS）である．

5. 構造的操作意味論（SOS）

最初に SOS のレシピの概略を述べておこう．

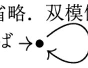
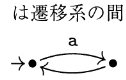
1. プロセス代数の各演算子の意味を **SOS ルール**として定義する．

2. 項の間の遷移関係 $s \xrightarrow{\mathsf{x}} t$ を，SOS ルールを用いて導出する．

3. 項を状態として，その間を上で導出された遷移関係でつないで得られる遷移系を意味として与える[*7]．

しばしば——具体的には SOS ルールの形が特定のフォーマットに従う場合——ステップ 2. の導出は項 s の構造に基づき帰納的に行われる．これが「構造的」操作意味論と呼ばれるゆえんである．

さっそくステップ 1. から：前節の Σ_{pa} に対して SOS ルールを与えよう．図 1 において，

*7) 本当は最後に「遷移系を**双模倣性**（bisimilarity）で割る」というステップがあるのだが，本稿では省略．双模倣性とは遷移系の間の同値関係の一つで，たとえば  と  を同一視する．

$$\frac{s \xrightarrow{\mathtt{x}} s'}{s \parallel t \xrightarrow{\mathtt{x}} s' \parallel t}\ (\parallel\mathrm{L}) \qquad \frac{t \xrightarrow{\mathtt{x}} t'}{s \parallel t \xrightarrow{\mathtt{x}} s \parallel t'}\ (\parallel\mathrm{R})$$

$$\frac{s \xrightarrow{\mathtt{x}} s'}{s + t \xrightarrow{\mathtt{x}} s'}\ (+\mathrm{L}) \qquad \frac{t \xrightarrow{\mathtt{x}} t'}{s + t \xrightarrow{\mathtt{x}} t'}\ (+\mathrm{R})$$

$$\frac{s \xrightarrow{\mathtt{x}} s'}{!\,s \xrightarrow{\mathtt{x}} s' \parallel !\,s}\ (!) \qquad \frac{}{\mathtt{x} \xrightarrow{\mathtt{x}} \mathbf{0}}\ (\textsc{AtomAct})$$

図 1 Σ_{pa} のための SOS ルール．

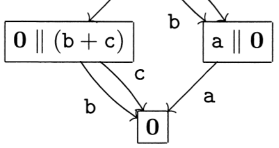
- $\mathtt{x}$ は $\mathtt{a}, \mathtt{b}, \mathtt{c}$ のいずれかを表し，s, s', t, t' は任意の Σ_{pa} 項を表す．
- ルールの横に書いてある $(\parallel\mathrm{L})$ や (AtomAct) はルールの名前である．「L」，「R」は左，右を表す．
- ルールは上から下に読む（「横線の上の遷移がすでに導出されたならば，そこからさらに横線の下の遷移を導出してよい」）．つまり，上が仮定で下が結論である．最後の (AtomAct) ルールには仮定がなく，これを導出におけるベースケースとして用いることができる．

4 節に述べた各演算子の「気持ち」が，SOS ルールとして表現されていることを納得してもらえるだろうか．たとえば項 s から $\mathtt{x}$ 遷移が可能であるとき（すなわち，ある s' に対して $s \xrightarrow{\mathtt{x}} s'$），項 $s \parallel t$ と $s + t$ の両方から $\mathtt{x}$ 遷移が可能であるが，前者では t が生き残る一方で，後者では t は忘れられてしまう．

ステップ 2. に進もう．遷移関係は SOS ルールを有限回用いて導出する．たとえば項 $\mathtt{a} \parallel (\mathtt{b} + \mathtt{c})$ において，$\mathtt{b} + \mathtt{c}$ が先に動作して，しかも $\mathtt{b}$ が選ばれた場合には $\mathtt{b}$ 遷移がおこるが，これは次のように SOS ルールを用いて導出される．

$$\cfrac{\cfrac{\cfrac{}{\mathtt{b} \xrightarrow{\mathtt{b}} \mathbf{0}}\ (\textsc{AtomAct})}{\mathtt{b} + \mathtt{c} \xrightarrow{\mathtt{b}} \mathbf{0}}\ (+\mathrm{L})}{\mathtt{a} \parallel (\mathtt{b} + \mathtt{c}) \xrightarrow{\mathtt{b}} \mathtt{a} \parallel \mathbf{0}}\ (\parallel\mathrm{R}) \tag{4}$$

項 $\mathtt{a} \parallel (\mathtt{b} + \mathtt{c})$ からはじめて，このような導出の可能なものをすべて挙げると次を得る．



(5)

最後にステップ 3. として，(5) において各状態に書いてある項を忘れると (3) の遷移系を得る．

図 1 の SOS ルールに対しては，(5) のように可能な遷移（すなわち，可能な導出）をすべて数え上げることはむずかしくない．なぜならば，各ルールにおいて仮定の左側は結論の左側の一部（**部分項**）になっているからである（たとえばルール $(\parallel\mathrm{L})$ において s は $s \parallel t$ の部分項）．よって (4) のような導出は，左側の項がだんだん「太っていく」形で行われる．

6. SOS の形式検証への応用

前節で，プロセス代数の項——すなわち，並列システムを表現する単純なプログラム——に対して (3) のような意味を定義する手法 SOS を紹介した．数学的・論理学的にはいかにもまっとうだが，計算機科学（特に本稿冒頭でふれた**形式検証**）ではこれをどのように**使う**のだろうか？

まず，現在の文脈で形式検証とは次の問題である．

- 入力 プロセス代数の項 t と，満たしてほしい性質 P．P の例は「$\mathtt{a}$ が現れたら，その後いつかかならず $\mathtt{b}$ が現れる」．
- 出力 項 t の表すシステム（すなわち遷移系 $[\![t]\!]$）が P を満たすか否か（Yes/No）．No の場合はできれば反例．

この問題は（主に経済的理由から）できれば自動化して解きたい：すなわち，形式検証問題を解くアルゴリズムを実装したいのである．

ここで図 1 によると，項 $!\,s$ は再帰呼び出しを行うゆえ，(2) のプログラムのように無限状態の遷移系をひきおこすことが多い．この場合には (3) のような意味を具体的に書きくだすのは不可能である（その前に我々の有限の寿命が尽きる）．

そこで多くの形式検証アルゴリズムは，項 t を遷移系 $[\![t]\!]$ に完全に展開することはせず，何らかの記号操作によって（記号列として与えられる）項 t と性質 P を変換していき Yes/No の出力に至る．そしてこのようなアルゴリズム——振り返ってみると文字列 t, P を機械的に変換しているだけである——が実際に形式検証問題を正しく解いているのかという問題は決して自明ではない．つまり「検証プログラム自体の（メタな）検証」が必要なのである．

この問題を（$[\![t]\!]$ を定義することで）定式化し，またその証明の手がかりを与えるのが，前節のような数学的意味論である．言いかえると，形式検証アルゴリズムの**メタ理論**（meta theory）を与えるのが数学的意

味論なのである．

また逆に，数学的意味論をスジよく発展させることで生まれる形式検証手法もある．たとえばプロセス代数の**要素還元性**（compositionality）とよばれる性質は「小さなシステムを部品として組み合わせて作った大きなシステムの性質は，部品それぞれの性質からわかる」ことをいい，次のように定式化される：各演算子 σ について

$$
\begin{aligned}
&[\![s_i]\!] \simeq [\![t_i]\!],\ \forall i \in [1,n] \quad \Longrightarrow \\
&\qquad [\![\sigma(s_1,\ldots,s_n)]\!] \simeq [\![\sigma(t_1,\ldots,t_n)]\!]. \quad (6)
\end{aligned}
$$

ここで $\simeq$ は遷移系の間の（何らかの意味での）等価性を表す*8)．たとえば「s_1 さんと t_1 さんの個人としての働きが同じで，s_2 と t_2 も同じであれば，s_1, s_2 二人のチームの働きは t_1, t_2 二人のチームの働きと同じ」という感じだが，現実にはむずかしそうだ：実は s_1 と s_2 は犬猿の仲であって，それぞれ個人として働いているうちには露見しなかっただけかもしれない．このような**予見しない内部干渉がない**という性質が要素還元性であり，複雑なシステムの形式検証をボトムアップに（部分部分から積み上げる形で）行うためには必要不可欠な性質である．

要素還元性は上記の（代数学に基づいた）SOS の格好のターゲットである：条件 (6) は，意味を与える写像 $[\![-]\!]$ が準同型写像であることに他ならない！*9)現在では要素還元性を保証するルールの形——5 節に述べたフォーマット——が多く研究され，たとえば図 1 のルールが要素還元性を満たすことは，あるフォーマットからすぐにわかる．

■ 7. おわりに ■

計算機科学（特に意味論）と代数学における**有限と無限の対比**，また**構文論と意味論の分離**についてインフォーマルに説明したのち，Plotkin の構造的操作意味論 SOS をかけ足で紹介した．SOS の入門は Aceto らによるもの[1]があるが，SOS の**圏論的代数・余代数**を用いた一般的な記述（Turi と Plotkin による）もエキサイティングでありオススメである（Klin による入門記事[2]がある）．論理学における構文論と意味論の分離

*8) たとえば脚注 7 で述べた双模倣性.

*9) 正確には：遷移系の $\simeq$ 同値類の上に演算子 σ の意味 $[\![\sigma]\!]$ が well-defined であり，かつ $[\![-]\!]$ が Σ 項の集合自身がなす代数からの準同型写像になっていること.

については，論理学の高級教科書である Shoenfield[3] が鬼軍曹のように鍛えあげてくれる．

本稿は計算機科学における意味論のわずかな一側面を語ったにすぎない．意味論の代表的な教科書は Winskel[4] であるが，プログラム意味論と幾何学的不変量のつながり[6]や，代数仕様を記述するための圏論的道具である**モナド**（monad）の計算機科学での使われ方[5]なども読者の興味のあるところであろう．

参考文献

1) L. Aceto, W. Fokkink and C. Verhoef. Structural operational semantics. In J. Bergstra, A. Ponse and S. Smolka, editors, *Handbook of Process Algebra*, pp.197–292. Elsevier, 2001.

2) B. Klin. Bialgebras for structural operational semantics: An introduction. *Theor. Comput. Sci.*, **412(38)**:5043–5069, 2011.

3) J.R. Shoenfield. *Mathematical Logic.* Addison-Wesley, 1967.

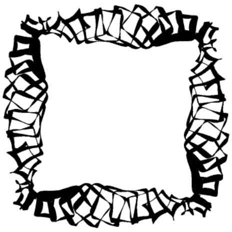
4) G. Winskel. *The Formal Semantics of Programming Languages.* MIT Press, 1993.

5) 勝股審也.「モナドと計算効果」圏論の歩き方（第 5 回），数学セミナー 2011 年 12 月号.

6) 長谷川真人.「プログラム意味論と圏論—計算の「不変量」を圏論で捉える」圏論の歩き方（第 4 回），数学セミナー 2011 年 11 月号.

（はすお・いちろう，東京大学大学院情報理工学系研究科）

力学系への代数的アプローチ



川口 周

1. 代数力学系への誘い

力学系は，広大な分野である．ここではその特別な場合を考えよう．X を集合として，$f: X \to X$ を X からそれ自身への写像とする．

X を相空間とみなし，時刻 $t=0$ の状態 $x \in X$ は，時刻 $t=1$ には状態 $f(x) \in X$ に移り，時刻 $t=2$ には状態 $f^2(x) := f(f(x)) \in X$ に移り，時刻 $t=n$ には状態 $f^n(x) \in X$ に移ると考えよう（ここで，$f^n: X \to X$ は f を n 回合成した写像を表す）．このとき，X と f の組 (X, f) は離散時間の自律系の力学系を記述すると考えられる．

X の元 x を一つ与える．このとき，x の **f-前軌道**（forward f-orbit）

$$x,\ f(x),\ f^2(x),\ f^3(x), \cdots \tag{1.1}$$

がどう振る舞うかを調べたくなる．

例えば，X に何らかの距離が入っているとき，与えられた元 x の f-前軌道の集合 (1.1) は有界な範囲に収まっているだろうか．

X の元 x は，$f^n(x) = x$ となる正の整数 n が存在するとき，**f-周期点**（f-periodic point）であるという．また，$f^n(x) = f^m(x)$ となる整数 $n > m \geq 0$ が存在するとき，**f-前周期点**（f-preperiodic point）であるという．このとき，与えられた元 x は f-周期点になるだろうか（時間がたつと初期状態 x に戻るだろうか）．あるいは，f-前周期点になるだろうか（同じ状態を繰り返すようになるだろうか）．

具体的な例として，X を複素数全体のなす集合 $\mathbb{C}$ とし，複素数 c を一つとり，$\mathbb{C}$ からそれ自身への写像として 2 次多項式 $f_c(z) = z^2 + c$ を考える．$X = \mathbb{C}$ の元として，$x = 0$ を与えよう．すると，0 の f_c-前軌道は，(1.1) で f を f_c，x を 0 とおいて，

$$0,\ c,\ c^2+c,\ (c^2+c)^2+c, \cdots \tag{1.2}$$

となる．

このとき，0 の f_c-前軌道 (1.2) が有界な範囲に収まるかどうかは，パラメータ c に依存する．そこで，(1.2) の点列が，$\mathbb{C}$ の中で有界となるようなパラメータ c からなる集合を

$$\mathcal{M} := \{c \in \mathbb{C} \mid (1.2) \text{ の点列は有界}\}$$

とおこう．ご存知の方も多いように，$\mathcal{M}$ は Mandelbrot 集合と呼ばれる．$f_c: \mathbb{C} \to \mathbb{C}$ が 2 次多項式で表される簡単と思われる写像であるにもかかわらず，$\mathcal{M}$ は極めて複雑な形をしている（図 1）[*1]．

さて，0 が f_c-前周期点であるかどうかも，パラメータ c に依存する．例えば，

$$c = -0.5 = -\frac{1}{2}$$

ととろう．このとき，0 の $f_{-0.5}$-前軌道は，(1.2)

*1） 図 1 と図 2 の画像は稲生啓行氏による．

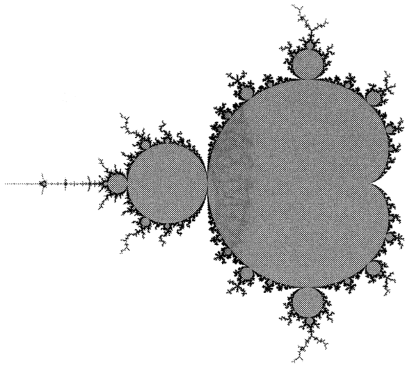


図 1　Mandelbrot 集合 $\mathcal{M}$.

に $c = -0.5$ を代入して，

$$0,\ -0.5,\ -0.25,\ -0.4375,\\ -0.30859\ldots,\ -0.40476\ldots,\ \cdots \quad (1.3)$$

となる．分数表示では，

$$0,\ -1/2,\ -1/4,\ -7/16,\\ -79/256,\ -26527/65536,\ \cdots \quad (1.4)$$

である．このとき，0 は $f_{-0.5}$-前周期点だろうか．

答えを先に述べると，0 は $f_{-0.5}$-前周期点ではない．このことを示す証明はいくつか考えられるが，一つの見易い証明は，小数表示 (1.3) ではなくて，分数表示 (1.4) に注目することである．(1.4) を見ると，$n = 1, 2, \cdots, 5$ に対して，

$$f^n_{-0.5}(0) = \frac{\text{奇数}}{2^{2^{n-1}}} \quad (1.5)$$

の形をしている．任意の $n \geq 1$ についても，(1.5) が成り立つことが，n に関する帰納法によって簡単に示せる．すると，整数 $n > m \geq 0$ に対して，$f^n_{-0.5}(0)$ と $f^m_{-0.5}(0)$ の既約分数表示の分母は異なるから，$f^n_{-0.5}(0) \neq f^m_{-0.5}(0)$ である．よって，0 は $f_{-0.5}$-前周期点ではない．

上の証明に，すでに，**力学系への代数的な（あるいは整数論的な）アプローチ**が現れている．取り上げた 2 次多項式 $f_{-0.5}(z) = z^2 - 1/2$ は，係数がすべて有理数なので，有理数体 $\mathbb{Q}$ 上で定義されている．このとき，$x = 0$ も有理数なので，0 の $f_{-0.5}$-前軌道に現れる点 $f^n_{-0.5}(0)$ はすべて有理数である．

さて，有理数の集合 $\mathbb{Q}$ は実数の集合 $\mathbb{R}$ に含まれる：

$$\mathbb{Q} \subset \mathbb{R}.$$

実際，$\mathbb{Q}$ の通常の絶対値 $|\cdot|$ から定まる距離に関する完備化が $\mathbb{R}$ である．

一方，p を素数とする．このとき，有理数が p のべきでどのくらい割り切れるかを考えることによって，$\mathbb{Q}$ には p-進ノルム $|\cdot|_p$ が定まる*2)．p-進ノルム $|\cdot|_p$ から定まる距離に関する完備化を p-進体といい $\mathbb{Q}_p$ で表す：

$$\mathbb{Q} \subset \mathbb{Q}_p.$$

まとめると次のようになる．

$$\boxed{\mathbb{R} \supset \mathbb{Q} \subset \mathbb{Q}_p}$$

小数表示 (1.3) が，有理数 $f^n_{-0.5}(0)$ を実数とみなす見方と思えば，2 のべきに注目した (1.5) は，有理数 $f^n_{-0.5}(0)$ を $\mathbb{Q}_2$ の元とみなす見方といえるだろう．実際，(1.5) は，$f^n_{-0.5}(0)$ の 2-進ノルムが $2^{2^{n-1}}$ であることを示していて，n, m が異なるとき，$f^n_{-0.5}(0)$ と $f^m_{-0.5}(0)$ の 2-進ノルムの値が異なるので，$f^n_{-0.5}(0) \neq f^m_{-0.5}(0)$ であるという議論をしている．

0 が $f_{-0.5}$-前周期点でないことを示したこの議論は，$f_{-0.5}$ の反復合成に関する性質を調べるときに，p-進体 $\mathbb{Q}_p$ を考えるアプローチがあることを示している．

離散時間の力学系は，実力学系，複素力学系と呼ばれるように，実数体 $\mathbb{R}$ や複素数体 $\mathbb{C}$ の上で考えられることが多い．しかし，上で述べたように，離散時間の力学系を，有理数体 $\mathbb{Q}$ や p-進体 $\mathbb{Q}_p$ の上で考えることもできる．

$\mathbb{Q}$ や $\mathbb{Q}_p$ など，$\mathbb{R}$ や $\mathbb{C}$ とは異なる体の上での

*2)　x が 0 でない有理数のとき，$x = p^n a/b$（n は整数，a, b は p と互いに素な整数）と表して，$|x|_p := p^{-n}$ と定める．$x = 0$ のときは，$|0|_p := 0$ と定める．

力学系は総じて，**代数力学系**（algebraic dynamics）と呼ばれる*3)．また，代数力学系よりはやや狭い意味で，有理数体 $\mathbb{Q}$ などの上の力学系は**数論力学系**（arithmetic dynamics），p-進体 $\mathbb{Q}_p$ などの上の力学系は**非アルキメデス的力学系**（non-Archimedean dynamics）と呼ばれる．

代数力学系や数論力学系の研究は，近年になり活発になされている*4)．本稿では，代数力学系の話題，あるいは，力学系への代数的なアプローチを 2 つ取り上げたい．

2. 力学系的次数

以下でも説明するように，射影空間の有理写像 $f : \mathbb{P}^k \dashrightarrow \mathbb{P}^k$ が与えられたとき，f を反復合成した有理写像 f^n の次数の増大度を，f の力学系的次数という．力学系的次数は，複素力学系と可積分系の研究者によって調べられてきた．この節では，力学系的次数について説明し，さらに力学系的次数への数論的なアプローチを紹介したい．

2.1 射影空間と有理写像

k 次元の（複素）射影空間は，商空間

$$\mathbb{P}^k = \left(\mathbb{C}^{k+1} \setminus \{0\}\right) / \sim$$

で定義される．ただし，$u, v \in \mathbb{C}^{k+1} \setminus \{0\}$ が $u \sim v$ であるとは，0 でない複素数 λ があって，$u = \lambda v$ となるときにいう．

$(x_1, x_2, \cdots, x_{k+1})$ の $\mathbb{P}^k$ における同値類を，$(x_1 : x_2 : \cdots : x_{k+1})$ で表す．

$f : \mathbb{P}^k \dashrightarrow \mathbb{P}^k$ が有理写像であるとは，f が

$$(x_1 : \cdots : x_{k+1})$$
$$\mapsto (F_1(x_1, \cdots, x_{k+1}) : \cdots : F_{k+1}(x_1, \cdots, x_{k+1}))$$

と表されるときにいう．ただし，$F_1, \cdots, F_{k+1}$ は $k+1$ 個の同じ次数の斉次多項式で，$F_1, \cdots, F_{k+1}$ の最大公約元は 1 であるものである．$F_1, \cdots, F_{k+1}$ の共通の次数を f の次数といい，$\deg(f)$ で表す．

なお，有理写像は，必ずしも射影空間全体 $\mathbb{P}^k$ で定義されているとは限らないことに注意しておく（そのため，写像 f を通常の矢印 $\longrightarrow$ ではなく，点線の矢印 $\dashrightarrow$ を用いて表している）．以下では，有理写像はその像の閉包が射影空間全体になるものを考える．

例 2.1. 2 次元射影空間 $\mathbb{P}^2$ は，比 $(x_1 : x_2 : x_3)$ のなす空間である．$\mathbb{P}^2$ 上の有理写像として，

$$f : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2,$$
$$(x_1 : x_2 : x_3) \mapsto \left(x_2 x_3 : x_1 x_2 : x_3^2\right)$$

を考える．$\deg(f) = 2$ である．f は点 $(1:0:0)$ と $(0:1:0)$ で定義されていない．

2.2 力学系的次数と代数的エントロピー

$f : \mathbb{P}^k \dashrightarrow \mathbb{P}^k$ を有理写像とする．このとき，

$$\delta_f := \lim_{n\to\infty} \sqrt[n]{\deg(f^n)} \tag{2.1}$$

を**力学系的次数**（dynamical degree）という*5)．

力学系的次数は複素力学系の研究者である Friedland–Milnor[4] や Russakovskii–Shiffman[8] たちによって導入された．

一方，可積分系の研究者である Bellon–Viallet[2] は，Russakovskii–Shiffman たちとは独立に，

$$\lim_{n\to\infty} \frac{1}{n} \log \deg(f^n)$$

という量を考え，この量を**代数的エントロピー**（algebraic entropy）と呼んだ．定義から，代数的エントロピーは $\log \delta_f$ に等しい．

ちなみに，複素力学系の研究者は，力学系的次数が 1 より大きい（すなわち，代数的エントロピーが正の）有理写像に興味がある一方，可積分系の研究者は，力学系的次数が 1 に等しい（すなわち，代数的エントロピーが 0）有理写像に興味があるように思われる．実際，Hietarinta–Viallet[5] は，f が可積分であることの必要条件として，代数的

*3) ただし，筆者は言葉遣いにそれほど自信がないことを断っておく．

*4) 例えば，アメリカ数学会による数学分野の分類 MSC2010 では，「37Pxx: Arithmetic and non-Archimedean dynamical systems」が追加された．

*5) 正確には，第 1 力学系的次数という．(2.1) の右辺の極限は収束する．

エントロピーが 0 であることを提唱している．

例 2.2. 例 2.1 の有理写像 $f:(x_1:x_2:x_3)\mapsto(x_2x_3:x_1x_2:x_3^2)$ について，力学系的次数を求めてみよう．例 2.1 で述べたように，$\deg(f)=2$ である．次に，

$$f^2((x_1:x_2:x_3))=(x_1x_2x_3^2:x_1x_2^2x_3:x_3^4)$$
$$=(x_1x_2x_3:x_1x_2^2:x_3^3)$$

となるから，$\deg(f^2)=3$ である[*6]．以下，同様に続けて，写像の反復合成の次数のなす数列

$$\deg(f),\ \deg(f^2),\ \deg(f^3),\ \deg(f^4),\ \cdots$$

は，

$$2,\ 3,\ 5,\ 8,\ 13,\ 21,\ \cdots$$

となる．これは Fibonacci 数列に他ならない．従って，f の力学系的次数 δ_f は，黄金比に等しいことが分かる：

$$\delta_f=\frac{1+\sqrt{5}}{2}.$$

Bellon–Viallet[2] は代数的エントロピーについて次の予想をたてた．

予想 2.1. 射影空間の有理写像 f の代数的エントロピーは，いつも代数的整数の対数である．言い換えれば，f の力学系的次数は，いつも代数的整数である．

ここで，最高次の係数が 1 の整数係数の多項式の根になる複素数を代数的整数という．

例えば，黄金比 $(1+\sqrt{5})/2$ は X^2-X+1 の根だから，代数的整数である．従って，例 2.1 の有理写像 f の力学系的次数は，確かに代数的整数になっている．

Bellon–Viallet の予想はいくつかの有理写像について確かめられているが，筆者の知る限り，一般には未解決である．

*6) 有理写像の次数の定義で，$F_1,\cdots,F_{k+1}$ の最大公約元は 1 にとっていたことに注意しよう．

2.3 有理点の高さと算術的次数

力学系的次数はその定義から代数的な雰囲気があるが，ここではさらに，力学系的次数への数論的なアプローチについて紹介したい．

そのために，まず，射影空間の点 $x=(x_1:x_2:\cdots:x_{k+1})$ が有理点のとき，すなわち，有理数の比で表されるとき，x の**高さ**（height）を定義しよう．射影空間の点は比で表されているので，$x_1,\cdots,x_{k+1}$ はいずれも整数で $x_1,\cdots,x_{k+1}$ の最大公約数は 1 であるとしてよい．このとき，x の高さ $h(x)$ を

$$h(x):=\log\max\{|x_1|,|x_2|,\cdots,|x_{k+1}|\}$$

で定義する．$h(x)$ は，x の算術的な大きさを測る量と考えられる．後の都合上，$h^+(x):=\max\{1,h(x)\}$ とおく．

例えば，$x=(1/2:1/3:1)$ は，$x=(3:2:6)$ と表されるから，x の高さは

$$h(x)=h((3:2:6))$$
$$=\log\max\{|3|,|2|,|6|\}=\log 6$$

となる．

さて，$f=(F_1:\cdots:F_{k+1})$ を k 次元射影空間の有理写像とし，多項式 $F_1,\cdots,F_{k+1}$ の係数はすべて有理数であるとする．また，有理点 x を一つとる．このとき，x の f-前軌道

$$x,\ f(x),\ f^2(x),\ f^3(x),\ \cdots$$

は，有理点の点列である[*7]．従って，その高さがどう振る舞うかを考えることができる．

$$\alpha_f(x):=\limsup_{n\to\infty}\sqrt[n]{h^+(f^n(x))}$$

とおいて，$\alpha_f(x)$ を x における f の**算術的次数**（arithmetic degree）と呼ぶ．

算術的次数と力学系的次数には次のような関係がある．

*7) すべての n について，$f^n(x)$ は f の定義域に入っていると仮定する．

定理 2.1.[7] 上の状況で，f の x における算術的次数 $\alpha_f(x)$ は，f の力学系的次数 δ_f を超えない．

さらに，x が一般的な点であれば，f の x における算術的次数 $\alpha_f(x)$ と力学系的次数 δ_f が一致することが予想されている．この予想を認めると，δ_f を計算するために，上手く初期値 x をとって，$\alpha_f(x)$ を計算することが考えられる（$\alpha_f(x)$ の計算のほうが一般に楽である）．

なお，力学系的次数 δ_f を調べるために，高さの増大度を調べるという考えは，非明示的ではあるが，Hirota–Kimura–Yahagi にすでに表れている[6]．

3. 等分布定理

数論力学系の深い定理に，**高さの小さい点の等分布定理**（equidistribution theorem for small height points）がある．この定理について簡単に紹介したい．

3.1 Julia 集合と平衡測度

$f(z) \in \mathbb{C}[z]$ を次数が 2 以上の多項式とし，$f(z)$ で定められる写像 $f : \mathbb{C} \to \mathbb{C}$ を考える．

$z \in \mathbb{C}$ の f-前軌道は，

$$z,\ f(z),\ f^2(z),\ f^3(z), \cdots$$

であった．

正確な定義は述べないが，次の性質をもつ $z \in \mathbb{C}$ を集めたものを，f の **Julia 集合**といい，$\mathcal{J}(f)$ で表す：z のいくらでも近い点で，その f-前軌道が z の f-前軌道とは大きく異なるものが存在する（図 2）．言い換えれば，f の Julia 集合は，誤差や近似に対して「不安定な」初期値からなる集合である．

さらに，$\mathcal{J}(f)$ に台を持つ $\mathbb{C}$ の正規化された測度 μ_f で，f の反復合成に関して良く振る舞うものが存在することが知られている．μ_f を f の**平衡測度**（equilibrium measure）という．

例 3.1. 例外的に簡単な場合であるが，$f_0(z) = z^2$ のときは，f_0 の Julia 集合 $\mathcal{J}(f_0)$ は単位円周 $S^1 = \{e^{i\theta} \mid \theta \in [0, 2\pi)\}$ に一致する．また，f_0 の平衡測度 μ_{f_0} は，S^1 上の $(1/2\pi)\,d\theta$ で与えられる．

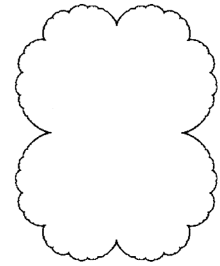


図 2　$z^2 + 1/4$ の Julia 集合．

3.2 高さの小さい点の等分布定理

有理数係数の 0 でない多項式の根になる複素数を代数的数という．上の $f(z) \in \mathbb{C}[z]$ について，その係数はすべて代数的数と仮定しよう．このとき，初期値 z も代数的数であれば，z の f-前軌道

$$z,\ f(z),\ f^2(z),\ f^3(z), \cdots$$

は，すべて代数的数になる．

$z \mapsto (z:1)$ という埋め込みによって，z を射影空間の点とみなすことができる．すると，2.3 節で述べたように，z が有理数のとき，z の高さ $h(z) := h((z:1))$ を考えることができる．さらに，z が代数的数のときも，z の高さ $h(z)$ を考えることができる．そこで，

$$\widehat{h}_f(z) := \lim_{n\to\infty} \frac{1}{\deg(f)^n} h\left(f^n(z)\right)$$

とおく*8)．$\widehat{h}_f(z)$ は f に関する z の標準的高さと呼ばれる．

さて，代数的数 z に対して，z を根にもつ有理数係数の多項式の中で次数が最小の多項式 $P(X)$ を考え，$P(X)$ の根全体を

$$G(z) := \{w \in \mathbb{C} \mid P(w) = 0\}$$

とおこう．言い換えれば，$G(z)$ は z の $\mathbb{Q}$ 上の共役元全体の集合である．例えば，$z = i$ のときは，

*8)　右辺の極限は収束する．

$P(X)$ は X^2-1 であり，$G(i)=\{i,-i\}$ である．

$G(z)$ が定める正規化された Dirac 測度を $\delta_{G(z)}$ とおく．すなわち，一点 w の Dirac 測度を δ_w で表せば，

$$\delta_{G(z)} := \frac{1}{\#G(z)} \sum_{w \in G(z)} \delta_w$$

である．

以上の準備の下で，等分布定理を述べよう．この場合（1 変数の多項式の場合）の定理は，Baker–Hsia による．

定理 3.1.[1] $f(z)$ は代数的数を係数とする次数が 2 以上の多項式とする．$\{z_m\}_{m=0}^{\infty}$ は相異なる代数的数からなる数列で，

$$\lim_{m\to\infty} \widehat{h}_f(z_m) = 0$$

をみたすとする．このとき，z_i の共役元全体 $G(z_m)$ が定める正規化された Dirac 測度 $\delta_{G(z_m)}$ は，$m\to\infty$ のとき，f の平衡測度 μ_f に弱収束する．

複素力学系では，周期が m の反発周期点の集合が定める正規化された Dirac 測度が，$m\to\infty$ のとき，f の平衡測度 μ_f に弱収束することが知られている．定理 3.1 は，このことの数論的な版とみることもできる．

定理 3.1 は，X. Yuan によってアラケロフ幾何を用いて，高次元の射影空間の場合も含む非常に一般的な形に拡張された[10]．Yuan の定理は，Mandelbrot 集合のようなパラメーター空間の数論的な性質を示すのにも応用されている[3]．

4. むすび

力学系への代数的アプローチの面白さを伝えられたか心もとないが，本稿では，力学系的次数と等分布定理の 2 つの話題を紹介した．この他にも，様々な方向への研究がなされている．最後に，この方面への入門書として，[Silverman][9] を挙げたい．

参考文献

1) M. Baker and L.-C. Hsia: Canonical heights, transfinite diameters, and polynomial dynamics, *J. Reine Angew. Math.* **585** (2005), 61–92.
2) M. Bellon and C. Viallet: Algebraic entropy, *Comm. Math. Phys.* **204** (1999), 425–437.
3) C. Favre and T. Gauthier: Distribution of postcritically finite polynomials, preprint arXiv:1302.0810.
4) S. Friedland and J. Milnor: Dynamical properties of plane polynomial automorphisms, *Ergod. Th. & Dynam. Sys.* **9** (1989), 67–99.
5) J. Hietarinta and C. Viallet: Singularity confinement and chaos in discrete systems, *Phys. Rev. Lett.* **81** (1998), 325–328.
6) R. Hirota, K. Kimura, H. Yahagi: How to find the conserved quantities of nonlinear discrete equations, *J. Phys. A: Math. Gen.* **34** (2001), 10377–10386.
7) S. Kawaguchi and J.H. Silverman: On the dynamical and arithmetic degrees of rational self-maps of algebraic varieties, preprint arXiv:1208.0815, accepted to *J. Reine Angew. Math.*
8) A. Russakovskii and B. Shiffman: Value distiribution for sequences of rational mappings and complex dynamics, *Indiana Univ. Math. J.* **46** (1997), 897–932.
9) J.H. Silverman: *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, **241**. Springer, New York, 2007. x+511 pp.
10) X. Yuan: Big line bundles over arithmetic varieties, *Invent. Math.* **173** (2008), 603–649.

（かわぐち・しゅう，京都大学大学院理学研究科）

炭素の新しい結晶 K_4 と代数学



小田　忠雄

はじめに

まず最初にお断りしておかなければならないが，“炭素の新しい結晶 K_4” が実在するか否かは現在のところ不明である．砂田[9]の表題にもあるように，自然が “創り忘れている” かもしれないのである．もっとも，合成の努力は続けられているようである．

小谷・砂田[1]において離散幾何解析における “エネルギー最小問題の解” として最も自然な形で結晶が定式化され，さらに，3次元空間における結晶の中で，ダイヤモンド結晶と K_4 結晶のみが**強等方性**という “美しさ” を有することが砂田[8~10]において数学的に証明されている．

炭素原子のみからなる結晶には，炭素原子がユークリッド平面に蜂の巣のような正6角形網目の形で結合しているグラフェン結晶があるが，この結晶での各炭素原子は3価であり，3本の結合手は同一平面上にある．一方ダイヤモンド結晶では，各炭素原子は4価であり，4本の結合手は立体的に拡がっている．ところが，炭素原子のみからなる K_4 結晶が存在するとすれば，各炭素原子がグラフェン結晶のように3価で，同一平面上にある3本の結合手でありながら，結晶全体としては立体的に構成されていることになる．このような結晶の可能性を見出したことで，数学の力が改めて認識されているようである．

本稿では，ダイヤモンド結晶や K_4 結晶等には “ボロノイ・タイル貼りが潜んでいる” ことが，代数幾何における “分類” の副産物として判明することをご紹介する．図4や図5で，ダイヤモンド結晶や K_4 結晶が全く新しい視点から眺められることをお判り頂けるであろう．果たして，物理的・化学的意味が何かあるであろうか？

1. 分類とは

本誌2013年10月号で「分類する《数理科学》：なぜ分けて考えるのか」が特集されたが，「分類」は数学において，また本稿においても重要な役割を果たすので，改めて採り上げてみたい．

数学での分類は，「同値関係」，「類別」，「商」という三位一体の概念である．大学教養教育までの数学では採り上げないので，数学科の学生諸君以外には馴染みが薄いと思われるが，数学において基本的な概念である．集合 S の要素の間の**同値関係** $\sim$ とは，次の3条件を満たすことである．

- （反射律）$x \sim x$ がすべての $x \in S$ に対して成り立つ．
- （対称律）$x, y \in S$ に対して，$x \sim y$ ならば $y \sim x$ が成り立つ．
- （推移律）$x, y, z \in S$ に対して，$x \sim y$ かつ $y \sim z$ ならば，$x \sim z$ が成り立つ．

S の要素が同じであると見なして分類する “基準” を与えるのである．S に同値関係を与えることは，S を，互いに交わらない部分集合 “類” の和集合

に分割する**類別**，すなわち

$$S=\bigcup_{i\in I}C_i,$$

かつ

$$i,j\in I,\quad i\neq j\quad \text{なら}\quad C_i\cap C_j=\emptyset$$

と同じである．同じ**同値類**C_iに属する要素$x,y\in C_i$を$x\sim y$と定義するのである．一方，各C_iを要素と見なす新しい**商集合**

$$S/\sim:=\{C_i\mid i\in I\}$$

と**上への写像**$\pi\colon S\twoheadrightarrow S/\sim$を，$x\in S$が$x\in C_i$のときに

$$\pi(x):=C_i$$

として定義できる．逆に，上への写像$\pi\colon S\twoheadrightarrow\overline{S}$が与えられれば，$x,y\in S$が$\pi(x)=\pi(y)$を満たすときに$x\sim y$とすれば，明らかに同値関係となる．各類$C_i$の要素$x_i$を選んだとき，$\{x_i\}_{i\in I}$を**完全代表系**と呼ぶ．$\pi$を$\{x_i\}_{i\in I}$に制限すると，

$$\pi\colon\{x_i\}_{i\in I}\to S/\sim$$

は，1対1で上への写像となる．

例えば，ベクトル空間Vとその部分空間Wとが与えられたとき，$x,y\in V$に対して

$$x\sim y\overset{\text{def}}{\iff}x-y\in W$$

と定義すれば，これはVでの同値関係である．この場合の商集合を普通V/Wと表す．V/Wには自然にベクトル空間の構造が入って剰余空間と呼び，上への写像$\pi\colon V\twoheadrightarrow V/W$は線形写像となる．数学科以外の学生諸君は，$V/W$の代わりに$V$における$W$の補空間$W'$を使うことを教えられているはずである．このとき$W'$は完全代表系の例である．

群Gが集合Xに右から作用するときの同値関係が後ほど必要になる．要素$x\in X$にGを作用させて得られる要素全体のなす**軌道**$xG:=\{xg\mid g\in G\}$が同値類であり，商集合をX/Gと記す．

2. 結晶とは

1984年の論文でShechtmanが“準結晶”の合成成功を報告し，国際結晶学連合が1992年に定義を変更するまで（Senechal[7]参照），結晶の定義は，周期性によるものであった．3次元ユークリッド空間で，数学的に理想化して言えば，原子が“離散的”かつ3つの独立した方向に関し周期的に分布しているのが結晶とされていた．本稿でも“**結晶**”と言えば，1991年以前の“古典的結晶”に限るものとする．結晶構造の従来からの分類は，3つの独立した周期から生成される周期格子と，適当に選んだ“単位胞”との組の持つ対称性によるものであり，代数学における群論が基本的な役割を果たしたことは，周知であろう．

しかし，ここでは，小谷・砂田[1]，砂田[8~10]による別の視点から結晶を考える．すなわち，n次元ユークリッド空間$\mathbb{R}^n$における結晶Gとは，原子を理想化した**頂点**どうしが結合手を理想化した**辺**で互いに結ばれて“離散的に”分布する**無限グラフ**であり，しかもn個の独立した方向に関して周期的であるものを考える．

Gを不変に保つ平行移動全体Lは，n次元ベクトル空間$\mathbb{R}^n$の格子である．そこで，Gに同値関係を導入しよう．Gの頂点は，Lに属する平行移動で互いに移るときに同値と見なす．また，Gの辺も，Lに属する平行移動で互いに移るときに同値と見なす．そうすると，この同値関係によるGの**商グラフ**G/Lが自然に考えられる．G/Lは，明らかに**有限グラフ**である．

例1（グラフェン結晶）　炭素原子がユークリッド平面に蜂の巣のような正6角形網目の形で結合しているグラフェン結晶Gの場合（図1左），商グラフG/Lは，2つの頂点を3本の辺で結んだグラフとなっている（図2右）．

3. 有限グラフのホモロジー群

$\{v_i\}_{i\in I}$を頂点集合，$\{e_j\}_{j\in J}$を辺集合とする

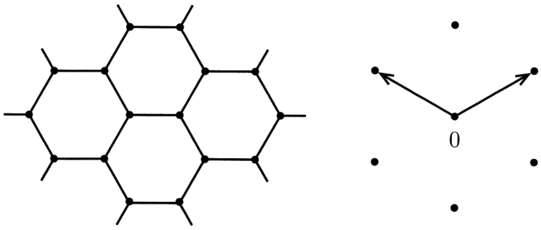


図 1　グラフェン結晶とそれを不変とする平行移動の格子.

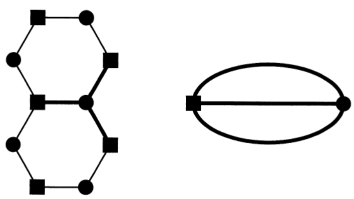


図 2　完全代表系とグラフェン結晶のグラフ $\Gamma = G/L$.

有限グラフを

$$\Gamma = \{\{v_i\}_{i\in I}, \{e_j\}_{j\in J}\}$$

とする．結晶から前記のようにして得られる有限グラフを考察の対象とするため，Γ は連結であるものとし，2 頂点を結ぶ辺が複数個あるものや，ある頂点と自分自身を結ぶループも許容する．Γ のホモロジー群 $H_1(\Gamma,\mathbb{Z})$, $H_1(\Gamma,\mathbb{R})$ を定義するため，各辺 e_j に任意の向きを与え固定しよう．e_j が頂点 v_i から頂点 $v_{i'}$ に向いた向きを与えられているとき，

$$s(e_j) := v_i, \quad t(e_j) := v_{i'}$$

と記す．

$\{v_i\}_{i\in I}$ を基底とする自由加群および実ベクトル空間を

$$C_0(\Gamma,\mathbb{Z}) := \bigoplus_{i\in I}\mathbb{Z}v_i, \quad C_0(\Gamma,\mathbb{R}) := \bigoplus_{i\in I}\mathbb{R}v_i$$

とし，$\{e_j\}_{j\in J}$ を基底とする自由加群および実ベクトル空間を

$$C_1(\Gamma,\mathbb{Z}) := \bigoplus_{j\in J}\mathbb{Z}e_j, \quad C_1(\Gamma,\mathbb{R}) := \bigoplus_{j\in J}\mathbb{R}e_j$$

とする．上記の向き付けを使用して**境界準同型**

$$C_0(\Gamma,\mathbb{Z}) \xleftarrow{\partial} C_1(\Gamma,\mathbb{Z}), \quad C_0(\Gamma,\mathbb{R}) \xleftarrow{\partial} C_1(\Gamma,\mathbb{R})$$

を，各 $j \in J$ に対して

$$\partial(e_j) := s(e_j) - t(e_j)$$

と定義する．このとき**ホモロジー群**は，境界準同型 ∂ の核として

$$H_1(\Gamma,\mathbb{Z}) := \{x \in C_1(\Gamma,\mathbb{Z}) \mid \partial x = 0\},$$
$$H_1(\Gamma,\mathbb{R}) := \{x \in C_1(\Gamma,\mathbb{R}) \mid \partial x = 0\}$$

と定義する．

簡単のため，

$$C := C_1(\Gamma,\mathbb{R}) \supset \Lambda := C_1(\Gamma,\mathbb{Z}),$$
$$H := H_1(\Gamma,\mathbb{R}) \supset H_{\mathbb{Z}} := H_1(\Gamma,\mathbb{Z})$$

と書くことにすると，Λ はベクトル空間 C の中の格子であり，$H_{\mathbb{Z}}$ はベクトル空間 H の中の格子である．

C は，$\{e_j\}$ を標準基底とする**内積**を

$$(e_j, e_{j'}) := \begin{cases} 1 & j = j', \\ 0 & j \neq j' \end{cases}$$

と定義すると，ユークリッド空間となり，その部分空間 H も自然にユークリッド空間となる．このとき直交射影を

$$\pi\colon C \to H$$

と記す．

4. 標準実現としての結晶

前節のような連結有限グラフ Γ が与えられたとき，関連する結晶をユークリッド空間の中で“美しい”（数学的にもっとも自然な）形で実現するのが，小谷・砂田[1)]の標準実現である．そのためには，まず Γ の**極大アーベル被覆グラフ**

$$\Gamma^{\mathrm{ab}} \longrightarrow \Gamma$$

を考える．Γ の頂点の一つ v_0 を基点として選んだとき，Γ^{ab} の要素は，Γ における $v_0 = v_{i(0)}$ か

らの**歩行** w

$$v_{i(0)} \xrightarrow{\varepsilon_{j(1)}e_{j(1)}} v_{i(1)} \xrightarrow{\varepsilon_{j(2)}e_{j(2)}} v_{i(2)} \longrightarrow$$

$$\cdots \xrightarrow{\varepsilon_{j(l)}e_{j(l)}} v_{i(l)} \longrightarrow \cdots \xrightarrow{\varepsilon_{j(m)}e_{j(m)}} v_{i(m)}$$

の“ある種の同値類” $\overline{w}$ である．ただし，$\varepsilon_{j(l)} = \pm 1$ であり，辺 e に対して $-e$ は辺に与えられた方向の逆方向の向きである，つまり

$$s(-e) = t(e), \quad t(-e) = s(e)$$

である．また，

$$t(\varepsilon_{j(l)}e_{j(l)}) = v_{i(l)} = s(\varepsilon_{j(l+1)}e_{j(l+1)})$$

がすべての $1 \leq l \leq m-1$ に対して成り立つものとする．

ホモロジー群 $H_{\mathbb{Z}}$ の要素は，v_0 から出て元の v_0 に戻る歩行である“サイクル”の一次結合であり，歩行の合成として $H_{\mathbb{Z}}$ は Γ^{ab} に作用し，その商グラフが

$$\Gamma^{\mathrm{ab}}/H_{\mathbb{Z}} = \Gamma$$

である．

Γ^{ab} のユークリッド空間 H における**標準実現**

$$\Phi\colon \Gamma^{\mathrm{ab}} \longrightarrow H$$

は，歩行 w に対応する Γ^{ab} の要素 $\overline{w}$ に対し，

$$\Phi(\overline{w}) := \sum_{l=1}^{m} \varepsilon_{j(l)}\pi(e_{j(l)})$$

となる．ただし，$\pi\colon C \to H$ は前述の直交射影である．$H_{\mathbb{Z}}$ の Γ^{ab} への作用および H への平行移動作用に関して，Φ は同変，つまり

$$\Phi(\alpha + \overline{w}) = \alpha + \Phi(\overline{w})$$

が $\alpha \in H_{\mathbb{Z}}$ および $\overline{w} \in \Gamma^{\mathrm{ab}}$ に対して成り立つ．

実はこの Φ は，離散幾何解析的なエネルギー最小問題の唯一の解となっているのである．詳しくは小谷・砂田[1)]，砂田[8~10)]を参照して頂きたい．

標準実現による像 $\Phi(\Gamma^{\mathrm{ab}})$ が，求める**結晶**であり，数学的にもっとも“美しい”．同変性から自然に導かれる写像

$$\Gamma = \Gamma^{\mathrm{ab}}/H_{\mathbb{Z}} \longrightarrow \Phi(\Gamma^{\mathrm{ab}})/H_{\mathbb{Z}}$$

は，Γ の“橋”を頂点につぶす以外には同型である．ただし，Γ の辺 e が**橋**であるとは，e を除去すると Γ が非連結になることである．

実は，Γ が橋を持たないことと，Γ に強連結な向き付けが可能なこととは同値である．ただし，向きづけられた有限グラフが**強連結**であるとは，任意の 2 点 v, v' が与えられたとき，v から各辺の向きに沿った歩行で v' に必ずたどり着けることを言う．

さらに，小谷・砂田[1)]は極大でない自由アーベル被覆グラフ $\widetilde{\Gamma} \to \Gamma$ に対する標準実現も考察するのであるが，紙数の関係でここでは割愛する．

5. $\boldsymbol{H}$ のボロノイ多面体

ユークリッド空間 C において原点を中心とする超立方体

$$V_J := \sum_{j\in J}\left[-\frac{1}{2}, \frac{1}{2}\right]e_j = \left\{\sum_{j\in J} y_j e_j \,\middle|\, -\frac{1}{2} \leq y_j \leq \frac{1}{2}, \forall j \in J\right\}$$

を考え，その $(\sum_{j\in J} e_j)/2 \in C$ による平行移動

$$D_J := \sum_{j\in J}[0,1]e_j = \left\{\sum_{j\in J} y_j e_j \,\middle|\, 0 \leq y_j \leq 1, \forall j \in J\right\}$$

も考える．

命題 2 直交射影 $\pi\colon C \to H$ による V_J の像 $\pi(V_J)$ は，格子 $H_{\mathbb{Z}}$ に関する 0 を中心とした**ボロノイ多面体**である．すなわち，

$$\pi(V_J) = \{x \in H \mid \|x\| \leq \|x - \alpha\|, \forall \alpha \in H_{\mathbb{Z}}\}$$

であり，$\pi(V_J)$ の $H_{\mathbb{Z}}$ による平行移動全体

$$\{\alpha + \pi(V_J)\}_{\alpha\in H_{\mathbb{Z}}}$$

は，互いに内部で交わらず，面と面がピッタリと接しながらに H を埋め尽くす**ボロノイ・タイル貼り**である．従って，それを平行移動した

$$\{\alpha + \pi(D_J)\}_{\alpha \in H_{\mathbb{Z}}}$$

も，互いに内部で交わらずに H を埋め尽くすタイル貼りである．

命題2で得られたボロノイ多面体 $\pi(V_J)$ は，Γ の強連結向き付け等と関連した数々の興味深い性質を持っている．詳細は小谷・砂田[2)]および拙著[5)]を参照して頂きたい．

6. タイル貼りに潜む結晶

定理3 H は2次元以上で，しかも Γ には橋がないと仮定する．そのとき，必要なら強連結となるように Γ の向き付けを変更し，さらに頂点 v_0 を適当に選べば，結晶 $\Phi(\Gamma^{\mathrm{ab}})$ には，タイル貼り

$$\{\alpha + \pi(D_J)\}_{\alpha \in H_{\mathbb{Z}}}$$

が "潜んで" いる，即ち，結晶はどのタイル $\alpha + \pi(D_J)$ の内部にも立ち入らず，表面のみにとどまる．

例4（グラフェン結晶） グラフェン結晶の場合に，グラフ Γ の強連結向き付けを図3左のように選んでみよう．このとき，

$$H_{\mathbb{Z}} = \mathbb{Z}(e_1 + e_3) \oplus \mathbb{Z}(e_2 + e_3)$$

である．簡単のため $\overline{e}_i := \pi(e_i)$ と書くことにすると，

$$\overline{e}_1 + \overline{e}_2 = \overline{e}_3$$

であり，ボロノイ多面体である正6角形の周囲を這うグラフェン結晶は図3右のようである．

例5（ダイヤモンド結晶） 炭素原子が3次元ユークリッド空間に分布している例の一つであるダイ

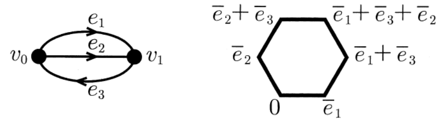


図3 グラフェン結晶の標準実現．

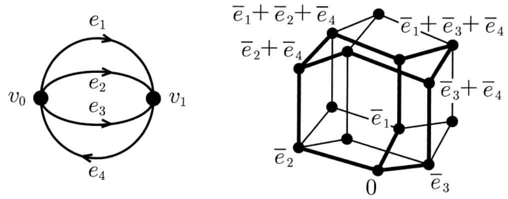


図4 ダイヤモンド結晶のグラフと，菱形12面体の表面を這う標準実現（太線部分）．

ヤモンド結晶 G の場合，商グラフ $\Gamma = G/L$ は，図4左のように，2つの頂点を4本の辺で結んだグラフとなっている．図のような強連結向き付けを選ぶと，

$$H_{\mathbb{Z}} = \mathbb{Z}(e_1 + e_4) \oplus \mathbb{Z}(e_2 + e_4) \oplus \mathbb{Z}(e_3 + e_4)$$

であり，簡単のため $\overline{e}_i := \pi(e_i)$ と書くことにすると

$$\overline{e}_1 + \overline{e}_2 + \overline{e}_3 = \overline{e}_4$$

となる．ボロノイ多面体は菱形12面体であり，その表面を這うダイヤモンド結晶は図4右の太線のようである．この菱形12面体をタイルとして3次元空間に敷き詰めてみると，ダイヤモンド結晶の各頂点にはちょうど4本の辺が集まっていることも想像に難くない．この場合の炭素は4価である．ダイヤモンド結晶の通常の図に較べて判り易いのではなかろうか．タイル貼りの利点である．

例6（K_4 結晶） 正4面体の頂点と辺からなる完全グラフ $\Gamma = K_4$ に，図5左のような強連結向き付けを与える．

$$H_{\mathbb{Z}} = \mathbb{Z}(e_2 + e_3 + f_1) \oplus \mathbb{Z}(-e_1 - e_3 + f_2) \oplus \mathbb{Z}(e_1 - e_2 + f_3)$$

である．簡単のため $\overline{e_i} := \pi(e_1)$, $\overline{f}_i := \pi(f_i)$ とすると，

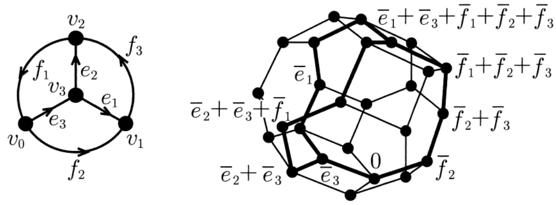


図 5　K_4 グラフと，ボロノイ多面体の表面を這う K_4 結晶の標準実現（太線部分）．

$$\overline{e}_1 = -\overline{f}_2 + \overline{f}_3,$$
$$\overline{e}_2 = \overline{f}_1 - \overline{f}_3,$$
$$\overline{e}_3 = \overline{f}_1 - \overline{f}_2$$

である．ボロノイ多面体は，切頭 8 面体であり，その表面を這う K_4 結晶の標準実現は，図 5 右の太線のようである．頂点 $\overline{e}_3$ に集まる 3 本の辺が同一平面上にあることに注目して頂きたい．実は，**標準実現の各頂点のいずれにも，同一平面上にある 3 本の辺が集まっている．**この切頭 8 面体をタイルとして 3 次元空間に敷き詰めるボロノイ・タイル貼りを部分的に組み立ててみると判る．砂田[9]の図とはまた違った形で K_4 結晶を理解できるのではなかろうか．

なお，極大でないアーベル被覆の場合の結晶で，類似の結果が適当な条件の下に成り立つか否かは現在のところ不明であり，究明中である．

ここまで，ホモロジー群程度の初歩的代数学しか登場していないが，本特集「数理科学における代数的構造：多彩な代数学的アプローチを探る」とどう関連するのかと疑問に思われるかも知れない．

実は，命題 2 は，“代数幾何における分類” を行った Seshadri との 1979 年の共同研究[6]の途中で見出したものなのである．

第 1 節の例で，ベクトル空間 V の部分空間 W による商 V/W も，自然にベクトル空間であることを見た．代数幾何における分類でも，考えている代数幾何学的対象の分類を，同値関係による商集合として実現するのが常で，しかもその商集合自身が代数幾何学的対象であることが多い．そのための有力な方法が**幾何学的不変式論**である．考えている代数幾何学的対象全体を，ある代数多様体における同値関係に関する**半安定点**全体の集合としてまず実現すると，商集合に自然な代数幾何学的構造が入るのである．

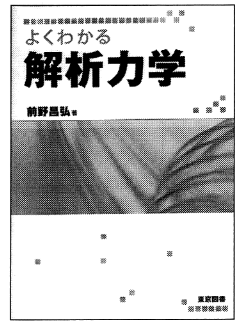
Seshadri との共同研究[6]で考察していたものが，結晶・準結晶の世界で**切断射影法**として知られているものに密接に関係していることが判明し，命題 2 および定理 3 に到達したのである．紙数の関係で，残念ながらこれ以上述べる余裕はない．最近の筆者の論文[5]末の簡単なまとめをご覧頂ければ幸いである．

参考文献

1) M. Kotani and T. Sunada, Standard realizations of crystal lattices via harmonic maps, *Trans. Amer. Math. Soc.* **353** (2000), 1–20.
2) M. Kotani and T. Sunada, Large deviation and the tangent cone at infinity of a crystal lattice, *Math. Z.* **254** (2006), 837–870.
3) T. Oda, Voronoi tilings hidden in crystals—the case of maximal abelian coverings—, *Tohoku Math. J.* **65** (2013), 1–30.
4) T. Oda, Convex polyhedral tilings hidden in crystals and quasicrystals, *RACSAM. Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A. Mat.*, **107** (2013), 123–143; DOI: 10.1007/s13398-012-0078-2.
5) T. Oda, Algebro-geometric stability and crystals *J. Ramanujan Math. Soc.* **28A** (Special Issue, July 2013), 353–408.
6) T. Oda and C.S. Seshadri, Compactifications of the generalized Jacobian variety, *Trans. Amer. Math. Soc.* **253** (1979), 1–90.
7) M. Senechal, What is a quasicrystal?, *Notices of Amer. Math. Soc.* **53**, No. 8, (2006), 886–887.
8) 砂田利一，『ダイヤモンドはなぜ美しい？—離散調和解析入門』，シュプリンガー・ジャパン，2006.
9) T. Sunada, Crystals that nature might miss creating, *Notices of Amer. Math. Soc.* **55**, No.2 (2008), 208–215.
10) T. Sunada, *Topological Crystallography: In View of Discrete Geometric Analysis*, Surveys and Tutorials in the Applied Mathematical Sciences Vol. 6, Springer-verlag, January 2013.

（おだ・ただお，東北大学名誉教授）

よくわかる解析力学



前野昌弘著，A5 判，384 頁，本体 2800 円，東京図書

本書は学部生向けの解析力学の教科書，自習書である．著者の前野昌弘氏は，弦理論，場の理論の専門家で…と紹介するよりは，ハンドル名“いろもの物理学者”というほうが話は通りやすい．ちなみに前野氏と筆者は同世代であり，同じ時期に京都でポスドクをやっていた．当時見かけるときはいつもジャージ姿であり，ざっくばらんな人であるとの印象を持っている．

本書を読むと，著者の人柄を表しているような，臨場感のある語り口を感じさせる．講義を聞いているようでもあり，説明は丁寧に何度でも繰り返し，時々間違えて戻りつつ進んでいく．また実際の講義同様に，少し説明が足りなくなってしまう箇所もあり，そこでは具体的に参考文献等を示してほしいと感じた．ちなみに本書で引用されている文献は姉妹書の『よくわかる初等力学』のみである．また図は工夫されているが書き込みすぎて見づらいものもある．こうしたことが気になった読者は Web 上で質問ができるサポートページが設けられてあるので覗いてはどうだろうか．そこでは誤植等の訂正をみることができる．私が気づいた誤植はホームページ上ではすでに訂正されていた．

本書の内容は，ニュートン力学の復習，変分法，仮想仕事と変分原理，ラグランジュ形式の解析力学，拘束系，連成振動，剛体の回転，保存則と対称性，ハミルトン形式の解析力学，相空間，ポアソン括弧，正準変換，ハミルトン・ヤコビ方程式という物理学を学ぶ学部学生にとって標準的な内容が含まれている．300 ページを越す厚さに対して内容は絞られており，例題，演習問題は基本的なものに限られているので，自習には演習書を別に必要とするであろう．また著者の専門を反映した用語（on-shell, off-shell）の使い方は他の学部生向けの本ではあまり見ない．筆者も個人的には，もう少し一般的になってほしいと思う用語である．

この本の序文にあるように，解析力学は 1 年次のニュートン力学を学んだ後の学生にとっては「得体のしれない学問」と感じる分野かもしれない．しかし，著者（筆者もそうであるが）も感じたように，量子力学，統計力学，場の量子論とより進んだことを学んでいく度に何度でもその面白さを味わえる学問でもある．それは物理学の体系を勉強していく際の一つの醍醐味であろう．本書は，その著者の学習体験を踏まえ，どのように理解すれば解析力学がわかりやすくなるかという工夫が凝らされている．その工夫の一つは，間違いやすい計算例を丁寧に説明してる点である．例えば，ラグランジアンの中に循環座標が含まれる場合のオイラー・ラグランジュ方程式の扱い（p.118）では，4 ページにわたり「失敗した」計算例が書いてある．筆者もこの部分について質問を受けるので，こういう例を丁寧に説明してくれると確かにわかりやすい．また FAQ というコラムではいろいろな種類の問いに著者が答えている．質問者は，「作用をわざわざ作る意味は何ですか？」とか「で，結局作用って何ですか」としつこく問うてきたり，「宇宙のエネルギーは保存しないのですか」という難しい問いを発したりする．著者は基本的には丁寧に答えているが，時には同じ説明を繰り返したりする回答もあり，おもしろい．読んでから 2 ページ目で作用の定義が現れる，名著ランダウ・リフシッツ理論物理学教程の『力学』の読者には予想もできない丁寧さである．ただし本書の帯にある「で結局ラグランジアンて何なのよ」という問いへの回答は書かれていないようである．“ランダウ・リフシッツ”を読み始めて挫折しそうな人，原理の「リクツ」について疑問をもった人は本書を読むと参考になることが多いと思われる．

これで“前野”理論物理学教程の一冊がまた完成した．前野節が好きな人は楽しめる本であると思う（ところで本家の理論物理学教程全巻の日本語訳は入手困難になっている．再見してみたいものである）．

伊藤　克司（東京工業大学大学院理工学研究科）

BOOK REVIEW

「数理科学」は語る

30年前から現代へのメッセージ

小柳　義夫

1984年5月号


数理科学

5

1984

MATHEMATICAL SCIENCES

特集 計算物理

計算物理とは	唐木幸比古
第三の物理学	有馬　朗人
格子ゲージ理論	小柳　義夫
原子核物理と数値計算	上村　正康
分子動力学法による剛体球系のシミュレーション	内藤　豊昭
数値固体物理…不規則系をとりあげて	吉野さやか
数値的相対論	中村　卓史
量子電気力学と高速数値計算	木下東一郎
《連載》パズル㊺ パズルのルールについて	高木　茂男
"我が太陽"を語る⑩	桜井　邦朋
生物のかたちづくり⑤	土居　洋文
FEM⑦ 有限要素法の誤差解析	菊地　文雄

No. 251

サイエンス社

物理学の進歩もすばらしいが，コンピュータの発展は桁違いである．記事の最後に書いたように，当時我々はメインフレーム計算機を使って格子ゲージ理論のシミュレーションを行っており，年間 CPU 時間が 2000 時間に達していた．高エネルギー物理学研究所（当時）のような恵まれた環境でもこれはほとんど限界であり，ヨーロッパにおいていくつかのスーパーコンピュータが使われ始めたと聞いて，いてもたってもいられない気持ちであった．

念願のスーパーコンピュータ HITAC S810/20 が東京大学大型計算機センターに設置されたのは，記事の前年であった．当時はプログラミングテクニックを駆使しないと高性能が実現しなかったので，多くのユーザは手をこまねいていた．我々はそのすきに自分たちのプログラムを高性能化し，どんどん走らせた．クォーク対の仮想的生成を無視するクエンチ近似であったが，$8^3 \times 16$ という当時としては大きな格子サイズのシミュレーションを行い，ハドロンの質量スペクトルを計算した．それでもハドロン 1 個を納めるには十分なサイズとは言えず，周期境界条件を用いているので，いわば「重箱に詰められたおはぎ」のようなハドロンを計算していたことになる．その後，7 つの大型計算機センターや研究所にスーパーコンピュータが続々設置され，格子ゲージ理論のみならず，様々な計算科学のための計算が行われた．

科学者の欲望は止まるところを知らない．いつでも今より 1000 倍高性能の計算機を欲しがるものである．記事には当時筆者らが格子ゲージ理論専用の超高速並列計算機の建設を考え始めていることを書いた．多くのコンピュータ科学者は，「アムダール則というのがあるから，高並列計算機は実用にならない．止めたほうがいいよ.」と親切に忠告してくれた．しかし私のいた筑波大学では qcdpax，cp-pacs，pacs-cs など計算科学のための超並列計算機を次々開発してきた．

日本では 1980 年代に国産のベクトル計算機が 3 社によって開発され，それがあまりに高性能だったので，ユーザは並列計算機に見向きもしなかった．アメリカでは同じ頃ベンチャービジネスにより多くの並列計算機が開発され，1990 年代には IBM と Cray が参入した．2000 年頃には並列計算について日本はアメリカより約 10 年遅れていたと思われる．

この状況を一変させたのが，理化学研究所が神戸に設置した「京コンピュータ」である．2011 年には 10.51 PFlops で世界一を達成し，翌年からは一般利用が開始された．これは 60 万並列の超高並列計算機であり，科学の多くの分野のみならず，産業界でも多くの成果を出している．30 年前を思うと昔日の感がある．

（おやなぎ・よしお，神戸大学大学院システム情報学研究科）

多層パーセプトロン(2)

特異構造と学習力学

甘利 俊一

連載の最終回として，特異点を含むモデルにおける統計的推論と学習のダイナミックスを述べて，幕を閉じたい．特異点を含むモデルの解析には高度の数学が必要である．ここではそれを避け，直観的に述べるに留めたい．また，パーセプトロンの学習力学は，まだ未完成なので，これも展望にとどめる．

30.1 特異モデルの幾何学

統計学の伝統的なモデル S は，n 次元のパラメータ $\boldsymbol{\xi}$ によって指定される確率変数 $\boldsymbol{x}$ の確率密度関数 $p(\boldsymbol{x}, \boldsymbol{\xi})$ の全体を対象とし，次の正則条件を課す．

1) $\boldsymbol{\xi}$ は n 次元ユークリッド空間の開集合に属する．

2) Fisher 情報行列が存在して，正則である．

このとき，モデル S は $\boldsymbol{\xi}$ を（局所）座標系とする多様体をなし，各点 $\boldsymbol{\xi}$ の接空間は，n 個の確率変数

$$u_i(\boldsymbol{x}, \boldsymbol{\xi}) = \frac{\partial \log p(\boldsymbol{x}, \boldsymbol{\xi})}{\partial \xi^i} \tag{30.1}$$

で張られる確率変数の線形空間と見なして良い．

以上の条件のもとで，Cramer–Rao の定理を中核とする，統計学の漸近理論の体系が築かれた．しかし，パーセプトロンを初めとする応用上重要な多くのモデルで正則条件が成立しない．このとき，特異性が現れ，通常の理論が成立しない．ここでは，特異モデルを議論するが，これを厳密に行うには解析学からの多くの準備が必要である．ここでは，何が起こっているのかを直観的に垣間見るが，詳しい理論は文献 1) を参照されたい．

特異性を持つモデルは，多層パーセプトロンだけではない．古くから，混合モデル，例えば混合ガウス分布が特異性を持つことが知られていた．この他，ナ

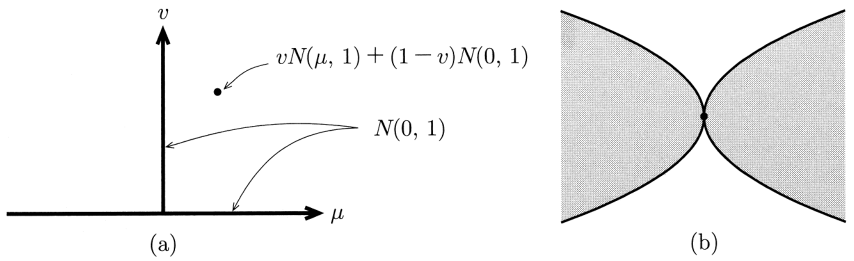


図 30.1　混合ガウス分布の特異領域.

イル河問題とも呼ばれる変化点モデル，隠れマルコフモデル，時系列の ARMA モデル，回帰分析の混合ガウス回帰モデルなどが特異性を持つ．ここでは，例として混合ガウス分布の特異モデルを使う．

混合型モデル

混合ガウス分布の族 M で，x の確率分布が

$$p\,(x,v,\mu) \sim vN(\mu,1)+(1-v)N(0,1) \tag{30.2}$$

となるものを考えよう．M は 2 つのガウス分布 $N(0,1)$ と $N(\mu,1)$ の混合分布から成り，パラメータは $\boldsymbol{\xi}=(v,\mu)$, $0\le v\le 1$, である．少し一般化して

$$p\,(x,v,\mu_1,\mu_2) \sim vN\,(\mu_1,1)+(1-v)N\,(\mu_2,1) \tag{30.3}$$

とすれば，もう少し面白い状況が分かるが，それにはあとで触れる．このモデルでは，異なるパラメータが同じ分布を指定することが起こるため，パラメータの同定不可能性が現れる．すなわち，図 30.1 (a) のパラメータの空間で，$\mu=0$ の軸上では v がどの値であっても分布は $N(0,1)$ である．また，$v=0$ の軸上では μ が何であっても分布は $N(0,1)$ である．したがって，これらの 2 直線上にあるパラメータはすべて同じ分布を示すから，これらの点は同値で

$$f_0(x)=N(0,1)=\frac{1}{\sqrt{2\pi}}\exp\left\{-\frac{1}{2}x^2\right\} \tag{30.4}$$

に等しい．この 2 直線が特異領域をなす．同値のものを一つにまとめた商空間 $M/\approx$ は，この 2 直線を 1 点にまとめるから，図 30.1 (b) のように見える．この点が特異点である．

特異点 $f_0(x)$ における接ベクトルを考えよう．特異点 $f_0(x)$ から出発し，$N(\mu,1)$ の成分が立ち上がる方向は，パラメータ t を用いて $\boldsymbol{\xi}(t)=(t,\mu)$, $0\le t$ という曲線である．ここで，μ は固定して考え，$N(\mu,1)$ の混合の度合 v が 0 から t まで増大する．この方向の接ベクトルは，確率変数で表示して

$$u(x,\mu)=\frac{d}{dt}\log p\left\{x,\boldsymbol{\xi}(t)\right\}\big|_{t=0}=\exp\left\{\mu x-\frac{1}{2}\mu^2\right\}-1 \tag{30.5}$$

である．これは μ 毎に違う．これはどの μ のところで v を 0 から立ち上げるかで，接ベクトルが違うからである．接ベクトルを定数倍した $cu(x,\mu)$, $c>0$, も接ベクトルであるから，その集合はコーンをなすが，線形空間にはならない．

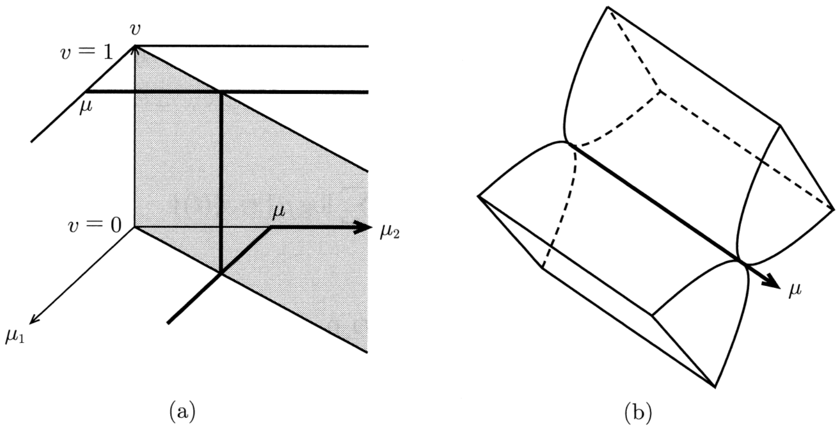


図 30.2　(30.3) 式のモデルの特異領域.

μ と μ' を異なる値とすると，$c_1 u(x,\mu) + c_2 u(x,\mu')$ を接ベクトルとする曲線 $\boldsymbol{\xi}(t)$ は存在しない.

接ベクトル全体の次元はいくつであろうか．$\mu_1, \cdots, \mu_m$ を異なる値とするとき，m 個の関数 $\exp(\mu_1 x), \exp(\mu_2 x), \cdots, \exp(\mu_m x)$ は関数の空間で 1 次独立である．これが任意 m について成立するので，この全体は有限次元に収まらない．パラメータが有限個なのに，なぜこのようなことが生ずるのであろうか．その秘密は特異点にある．$v = 0$ の特異点で，どの $N(\mu, 1)$ 成分を増やしても接ベクトルが得られるが，それらは皆違う．μ は連続パラメータであるから，このような接ベクトルは無限個あって，1 次独立である．つまり，$v = 0$ で特異領域が μ をパラメータとする連続領域をなし，そのどこからも接ベクトルが立ち上がるので無限次元が現れる.

ここで，少し拡大したモデル (30.3) を見よう．このモデルでは，各 μ に対して，$\mu_1 = \mu_2 = \mu$ もしくは，$v = 0$ で $\mu_2 = \mu$，同じく $v = 1$ で $\mu_1 = \mu$ という 3 つの線が，同一の分布 $N(\mu, 1)$ を表し，同定不能である（図 30.2 (a)）．これを同値類とすると，商空間は，これを一点に縮めたものである．このような同値の領域が各 μ ごとに存在して，それが連続につながっている．その全体が特異領域である．商空間 $M/\approx$ で考えれば，各 μ に対応する特異点は分布 $N(\mu, 1)$ に対応し，これが連続につながって線になっている（図 30.2 (b)）．これが $M/\approx$ における特異点の集合である．特異点における接ベクトルは各 μ 毎にコーンをなし，無限次元である.

30.2 対数尤度比と最尤推定量

(30.2) のモデルに戻り，真の値が特異点 $f_0(x)$ にある時の最尤推定を考える．観測されたデータ $D = \{x_1, \cdots, x_N\}$ に対して，対数尤度比

$$L(\boldsymbol{\xi}) = \sum_{i=1}^{T} \log \frac{f(x_i, \boldsymbol{\xi})}{f_0(x_i)} \tag{30.6}$$

を考えよう．これを最大にする $\boldsymbol{\xi}$ が最尤推定量である．特異点の近傍の $\boldsymbol{\xi}$ のうち，特定の μ に対応する接ベクトル方向をまず考える．$N(\mu,1)$ 方向の成分が立ち上がる曲線を $\boldsymbol{\xi}(t,\mu)$ として，この線上での最尤推定量 $\hat{v}(\mu)$ を計算しよう．t を微小として

$$l\left\{D,\boldsymbol{\xi}(t)\right\} = \sum \log p\left\{x_i,\boldsymbol{\xi}(t)\right\} \tag{30.7}$$

を展開すれば，

$$l(D,t,\mu) = l(D,0,\mu) + l'(D)t + \frac{1}{2}l''(D)t^2 \tag{30.8}$$

となる．ここで大数の法則により，$l''(D)/N$ はこの方向の Fisher 情報量 $g_{vv}(\mu)|_{v=0}$ に収束する．また，

$$\frac{1}{\sqrt{N}}l'(D) = \frac{1}{\sqrt{N}}\sum_{i=1}^{N} u\left(x_i,\mu\right) \tag{30.9}$$

は，中心極限定理により，平均 0，分散 $g_{vv}(\mu)$ のガウス分布である．確率変数

$$\tilde{u}(x,\mu) = \frac{u(x,\mu)}{\sqrt{g_{vv}(\mu)}} \tag{30.10}$$

は各 μ に対して平均 0，分散 1 のガウス分布である．

(30.8) を t で微分して 0 と置けば，μ を固定した曲線上 $\boldsymbol{\xi}(t,\mu)$ での最尤推定は $\hat{v}_\mu = -l'(D)/l''(D)$ となる．これを (30.8) に代入すれば，

$$l\left(D,\hat{v}_\mu,\mu\right) = l(D,0) + u(D,\mu)^2, \quad u(D,\mu) = \frac{\sum l'\left(x_i,\hat{v}_\mu,\mu\right)}{\sqrt{g_{vv}(\mu)}} \tag{30.11}$$

が得られる．最尤推定量は，$l\left(D,\hat{v}_\mu,\mu\right)$ を最大にする μ の値 $\hat{\mu}$ とそこでの $\hat{v}_{\hat{\mu}}$ である．これより次式を得る．

$$\hat{\mu} = \arg\max u(D,\mu)^2, \quad L\left(D,\hat{\boldsymbol{\xi}}\right) = \max_{\mu}\left\{u(D,\mu)\right\}^2. \tag{30.12}$$

$u(x,\mu)$ は，1 次元の場 μ 上で定義されたガウス分布の場で，その分散は 1，$u\left(x,\mu_1\right)$ と $u\left(x,\mu_2\right)$ の共分散は $\sigma^2_{\mu_1\mu_2} = E\left[u\left(x,\mu_1\right)u\left(x,\mu_2\right)\right]$ である．だから，この特異分布モデルの対数尤度比の分布は，ランダムガウス確率場の最大値 (30.12) の 2 乗の分布になる．いま，場 μ でほぼ独立なものが，$u\left(x,\mu_1\right),\cdots,u\left(x,\mu_m\right)$ の m 個とれたとしよう．このとき極限極値分布の理論により，

$$E\left[\max_{\mu}\left\{u(x,\mu)\right\}^2\right] = 2\log m \tag{30.13}$$

であることが分かっている．したがって，このモデルにおける対数尤度比は，N が増えるにつれて，確率場において独立なものがどのくらいの数とれるかという計算に帰着する．正則なモデルにおいては，パラメータ $\boldsymbol{\xi}$ の次元を d とすると，これは自由度 d の χ^2 分布に従い，その期待値が d である．特異の場合，これはそう簡単には計算できないが，混合ガウス分布の場合は $\log\log N$,

パーセプトロンの場合は $\log N$ のオーダーになることが福水によって証明された[1,2]．これは N と共に無限大に発散する．これにより，推定や検定の漸近的な特性は，Cramer–Rao 則に従う正規な場合とは大変違ったものになる．

30.3 多層パーセプトロンの学習力学

特異領域は学習の動特性に大きな影響を及ぼす．パーセプトロンを考えよう．多層パーセプトロンで，中間層の素子が 2 個の場合，入出力関係は

$$y = f(\boldsymbol{x}, \boldsymbol{\xi}) + n = v_1 \varphi(\boldsymbol{w}_1 \cdot \boldsymbol{x}) + v_2 \varphi(\boldsymbol{w}_2 \cdot \boldsymbol{x}) + n \tag{30.14}$$

となる．パラメータは $\boldsymbol{\xi} = (\boldsymbol{w}_1, \boldsymbol{w}_2, v_1, v_2)$ であるが，特異領域

$$R = \{\boldsymbol{\xi} \mid v_1 v_2 |\boldsymbol{w}_1 - \boldsymbol{w}_2| = 0\} \tag{30.15}$$

を持つ．このモデルの学習の方程式で特異点の近くでのダイナミックスを解析し，特異点が学習の軌道にどのような影響を与えるかを調べよう[3]．なお，中間層の素子が 2 個の場合は簡単すぎて一般性がないと思うかもしれないが，中間層の素子が多数ある場合も，特異性が現れるのは，2 個の素子の重み $\boldsymbol{w}_1$ と $\boldsymbol{w}_2$ が等しくなる場合（素子融合による特異点）と $v_i = 0$ となる場合（素子消失による特異点）の 2 つが通常である．3 個の素子もしくはそれ以上の素子で $\boldsymbol{w}_i$ が同時に等しくなるという縮退した場合もあり得るが，それはまれであるから，とりあえず 2 個の素子で重みベクトルが一致する場合，またはどれか 1 個の素子の v_i が 0 になる場合を調べておけばよい．

学習で更新するパラメータは $\boldsymbol{\xi} = (\boldsymbol{w}_1, \boldsymbol{w}_2, v_1, v_2)$ である．通常の勾配学習は

$$\boldsymbol{\xi}_{t+1} = \boldsymbol{\xi}_t - \eta \frac{\partial l(\boldsymbol{x}_t, y_t, \boldsymbol{\xi}_t)}{\partial \boldsymbol{\xi}} \tag{30.16}$$

という確率差分方程式である．ここで，解析を容易にするために，連続時間の方程式を用いることにする．入力 $\boldsymbol{x}_t$ がある確率分布からランダムに発生するものとすると，確率項はその期待値を取って，平均学習方程式

$$\dot{\boldsymbol{\xi}}(t) = -\eta \left\langle \frac{\partial l(\boldsymbol{x}, y, \boldsymbol{\xi}(t))}{\partial \boldsymbol{\xi}} \right\rangle \tag{30.17}$$

が得られる．$\langle\ \rangle$ は入力信号 $\boldsymbol{x}$ と教師信号 y についての期待値である．ここで，$\boldsymbol{x}$ の確率分布はガウス分布 $N(0, I)$ を仮定する．さらに，非線形のシグモイド関数として，誤差積分関数

$$\varphi(u) = \sqrt{\frac{2}{\pi}} \int_0^u \exp\left\{-\frac{s^2}{2}\right\} ds \tag{30.18}$$

を用いる．これも，式を解析的に求めるための細工である．

学習方程式の解の挙動に特異点がどう影響するかを解析する[4~6]．特異点の近傍での学習状況を明らかにするには，座標変換をして

$$\boldsymbol{u} = \boldsymbol{w}_2 - \boldsymbol{w}_1, \quad \boldsymbol{s} = \frac{v_1 \boldsymbol{w}_1 + v_2 \boldsymbol{w}_2}{v_1 + v_2}, \tag{30.19}$$

$$z=\frac{v_1-v_2}{v_1+v_2},\quad r=v_1+v_2 \tag{30.20}$$

と置く．この座標系では，特異領域 R は $\boldsymbol{u}=0,\quad z=\pm 1$ になる．

平均学習方程式を新しい座標系で書くには (30.17) を新しい座標系 $\boldsymbol{\zeta}=(\boldsymbol{u},z,\boldsymbol{s},r)$ で書き直す．座標変換 (30.19)–(30.20) のヤコビ行列を T とすれば，学習方程式は

$$\dot{\boldsymbol{\zeta}}=-\eta TT'\left\langle\frac{\partial l(\boldsymbol{x},y,\boldsymbol{\zeta})}{\partial\boldsymbol{\zeta}}\right\rangle \tag{30.21}$$

となる．特異領域 R を $R_1=\{\boldsymbol{u}=0\}$，$R_2=\{z=\pm 1\}$ の 2 つに分ける．R_1 は 2 個の中間層の素子の一致する場合であり，R_2 はどちらかの素子で，出力層へ入るときの重みが 0 になる場合である[4~6)]．

特異点の近傍，すなわち $\boldsymbol{u}=0$ もしくは $z=\pm 1$ の近くで，パラメータ $\boldsymbol{\zeta}$ を用いて書いた出力関数 $f(\boldsymbol{x},\boldsymbol{\zeta})$ がどう振る舞うかを調べておこう．関数 $f(\boldsymbol{x},\boldsymbol{\zeta})$ は

$$\begin{aligned}f(\boldsymbol{x},\boldsymbol{\zeta})\;=\;&\frac{1}{2}r(1+z)\varphi\left\{\boldsymbol{x},\boldsymbol{s}+\frac{1}{2}(z-1)\boldsymbol{u}\right\}\\&+\frac{1}{2}w(1-z)\varphi\left\{\boldsymbol{x},\boldsymbol{s}+\frac{1}{2}(z+1)\boldsymbol{u}\right\}\end{aligned} \tag{30.22}$$

になる．これを $\boldsymbol{u}$ についてテイラー展開すれば，$\boldsymbol{u}$ の 3 乗以上の項は省略して

$$f(\boldsymbol{x},\boldsymbol{\zeta})=w\phi(\boldsymbol{x},\boldsymbol{s})+\frac{1}{8}\left(1-u^2\right)\boldsymbol{u}'J\boldsymbol{u},\quad J=\frac{\partial^2\varphi(\boldsymbol{x},\boldsymbol{s})}{\partial\boldsymbol{s}\partial\boldsymbol{s}} \tag{30.23}$$

となる．これを使って，平均学習方程式を具体的に書き直すことができる．

ところが，変数 $\boldsymbol{s},r$ に関する方程式は特異性を含まない普通の形をしていて，これらの変数はすぐに安定平衡状態に近づく．その形を具体的に書くこともできるが，わずらわしいだけなので省略しよう．問題となるのは，特異領域の近傍での学習における $\boldsymbol{u},z$ の振舞いである．他のパラメータは収束したものとし，これらの変数の方程式を具体的に書くと

$$\dot{\boldsymbol{u}}\;=\;2\left(1-z^2\right)H\boldsymbol{u}, \tag{30.24}$$

$$\dot{z}\;=\;-\frac{z\left(1-z^2\right)}{r^2}\boldsymbol{u}'H\boldsymbol{u}-\frac{2z(z+1)}{r^2}\boldsymbol{u}'H\boldsymbol{u} \tag{30.25}$$

のようになる．ただし

$$H=\frac{r}{4}\left\langle(y-f(\boldsymbol{x},\boldsymbol{y}))\frac{\partial^2\varphi}{\partial\boldsymbol{s}\partial\boldsymbol{s}}\right\rangle \tag{30.26}$$

で，r は v_1+v_2 の収束した値である．方程式をつぶさに調べれば，特異領域 $R=R_1\cup R_2$ では，$\dot{\boldsymbol{\zeta}}=0$ が成立し，これが学習方程式の平衡点であることが分かる．しかし，その安定性を調べるには H の固有値を調べなければならない．計算を進めると，平衡点の安定性に関わる次の定理が得られる[4~6)]．

定理 30.1　教師信号の持つ真の解が特異領域上にあるときは，R_1 は安定平衡点の集まりである．真の解が特異領域上にないときは，H の固有値によって次の 3 つの場合に分かれる．

1)　固有値が正と負の値を持つ場合：特異点はすべて不安定．

2)　固有値が 2 つとも負の場合：R_1 のうち，$|z| < 1$ を満たす部分が安定．

3)　固有値が 2 つとも正の場合：R_1 のうち，$|z| > 1$ を満たす部分が安定．

さらに，R_1 の特異点の近傍の解析を進める．エネルギー関数 $h(\boldsymbol{u}) = 0.5|\boldsymbol{u}|^2$ を導入しよう．これは，現在の状態 $\boldsymbol{\zeta}$ が特異領域 R_1 からどのくらい離れているかを計る量である．これを微分すると

$$\dot{h}(\boldsymbol{u}) = \boldsymbol{u}'\dot{\boldsymbol{u}} = \frac{2r^2\left(z^2-1\right)}{z\left(z^2+3\right)}\dot{z} \tag{30.27}$$

が得られる．この方程式は積分できて，積分曲線は c を任意定数として

$$h(\boldsymbol{u}) = \frac{2r^2}{3}\log\frac{\left(z^2+3\right)^3}{|z|} + c \tag{30.28}$$

である．これが，学習の解の軌道であり，特異領域 R_1 の近傍での学習のダイナミックスを記述する．

ここで，もう一つの特異領域 R_2 の近傍も併せて，$R_1 \cap R_2$ の近傍では，

$$\dot{h} = \frac{r^2\left(z^2-1\right)}{z\left(z^2+1\right)}\dot{z} \tag{30.29}$$

が成立する．したがって，解の軌道は次の定理で与えられる．

定理 30.2　特異領域 R_1 の近傍では，学習方程式の軌道は

$$h(\boldsymbol{u}) = \frac{r^2}{3}\log\frac{\left(z^2+3\right)^2}{|z|} + c. \tag{30.30}$$

さらに，$R_1 \cap R_2$ では

$$h(\boldsymbol{u}) = r^2\log\left(|z| + \frac{1}{|z|}\right) + c. \tag{30.31}$$

解の軌道を 3 つの場合に分けて図 30.3 に与える．(A) は，真の解が特異領域上にある場合で，この場合，学習する生徒のパーセプトロンは実は 1 個の中間素子を持てば十分であった．解の軌跡は図 30.3 (A) に示すように，真の解のどこかへ収束していく．ただし，収束の速度は大変遅い．これは，自然勾配法を使うと著しく改善される．真の解が特異集合上にはなく，これを実現するのに中間素子 2 個が必要な場合を考えよう．このとき，行列 H の固有値の正負によって，3 つの場合に分かれる．固有値が正と負の 1 つずつのときは，R_1 は不安定である．したがって，解はここへは近づかないから，心配はいらない．他の 2 つの場合は固有値の符号が一致している．このとき，固有値が 2 つとも負ならば，R_1 上で $|z| < 1$ の区間が安定になる．したがって図 30.3 (B) に見るように，解軌道は初期値がある範囲にある場合，一度は R_1 の安定領域に入る．学

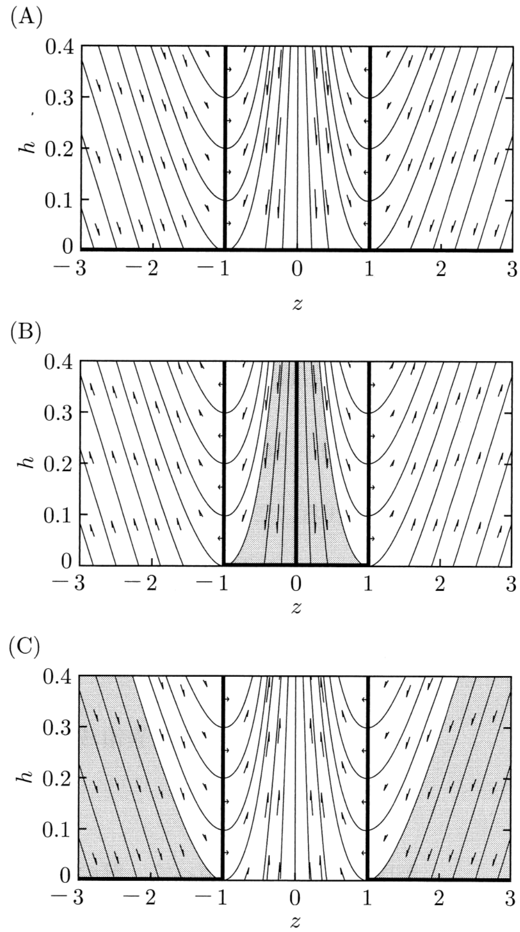


図 30.3　特異領域の近傍における学習の軌道：(A) 真の解が特異領域にあるとき，(B) $|z| < 1$ が安定領域であるとき，(C) $|z| > 1$ が安定領域であるとき．

習は入力 x が確率的に出現するので確率的な変動を伴う．このため，学習により $\boldsymbol{\xi}_t$ は R_1 の $|z| < 1$ の領域上をランダムウォークをする．実際は，$\boldsymbol{u}$ が 0 から少しずれたところで系統的な流れの成分が生じ，区間の両端に行く．ここを超えると R_1 は不安定である．したがって，特異領域から急速に出ていく．H の固有値が共に正である場合は，図 30.3 (C) のように，R_1 の $|z| > 1$ の領域が安定で，一度ここに入ってから，ランダムウォークで $|z| = 1$ の区間に到達し，ここから出ていく．これらの場合，特異領域のアトラクターは有限の測度の収束域を持ち，一度ここに入ってから出ていくという意味で Milnor attractor[7] になっている．これが人々を悩ませたプラトーと呼ばれる現象の本体である．

学習が遅滞するのに 2 つの場合があった．一つは真のモデルと生徒のモデルとで中間素子の数が違い，真のモデルのほうが少ない数の素子で実現できて，生徒は無駄な素子を含んでいる場合である．このとき，真の分布は特異領域にある．通常のバックプロパゲーション学習では，パラメータが特異領域に入るまで大変時間がかかった．自然勾配学習法ではこれが解消し，真の解が特異領域に

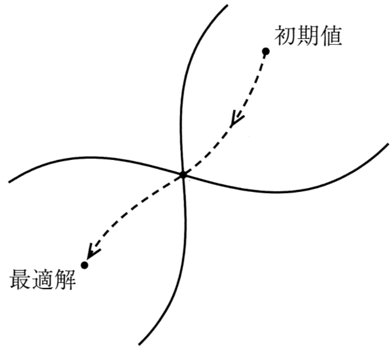


図 30.4　特異点を経由する学習軌道.

ある場合でも，通常の速度で特異領域に落ち込む．この場合の解析が Cousseau らによって与えられている[5]．もう一つは，真の分布は通常の領域にあるにも関わらず，学習の軌跡が特異点に引き込まれ，ここから抜け出すのに時間がかかる場合である．例えば，商空間が図 30.4 のようであったとしよう．真の解と，初期値とが特異点をまたいで異なる領域にあれば，学習は必然的に特異点を超えることになる．通常の学習ではここで遅滞が起こる[4,6]．自然勾配法でも特異点を超えるが，それは通常の場合と同じ速度で難なく超えるから，遅滞が起こらない．この場合の解析は，これからの課題である．

30.4 Bayes 推論と特異点

これまで，特異モデルにおける対数尤度比と最尤推定量の奇妙な振舞いを見てきた．Bayes 推論は，事前分布を用いてデータからパラメータの事後確率分布を計算する．これを最大にするのが MAP 推定量 $\hat{\boldsymbol{\xi}}_{\mathrm{MAP}}$ である．しかし Bayes 推論の性能は，事前分布に依存するため，良い事前分布を用いることができれば性能が上がる．正則なモデルで，パラメータ空間上の滑らかな事前分布 $\pi(\boldsymbol{\xi})$ を選べば，π として何を選ぼうとその効果は観測数 N とともに減少し，MAP 推定量は最尤推定量に収束する．

ところが特異モデルでは，パラメータ空間上の滑らかな事前分布 $\pi(\boldsymbol{\xi})$ は，商空間 $M/\approx$ 上の滑らかな事前分布と一致しない．特異モデルの特異領域では，一つの同値類上は $\boldsymbol{\xi}$ が違っても分布は同じである．同じ分布を与える $\boldsymbol{\xi}$ は無限個あるから，商空間の事前分布は無限個の点の重みを加えたものになる．このため，パラメータ空間上の滑らかな分布は商空間上では特異点に事前確率が集中する特異分布となる．したがって，Bayes 推論は特異領域に有利に作用する．特異領域は階層モデルで次数の少ないモデルに対応するため，AIC や MDL のように次数に応じた罰金項を付けなくても，自然にモデル選択が行えて，次数の多くないモデルが選択される．しかし，この選択が最適という保証はない．

パーセプトロンなどにおける学習は，入力 $\boldsymbol{x}$ に対して，出力 $y = f(\boldsymbol{x}, \boldsymbol{\xi})$ を出す関数のパラメータ $\boldsymbol{\xi}$ をデータから学習で求めることであった．データ

$D_N = \{(\boldsymbol{x}_1, y_1), \cdots, (\boldsymbol{x}_N, y_N)\}$ に基づく予測分布（新しい入力 $\boldsymbol{x}$ に対する条件付きの y の分布）$p(y|\boldsymbol{x})$ が Bayes の定理を用いて求まる．ここで，すべての量は入力 $\boldsymbol{x}$ の条件付きだから，簡単のため $\boldsymbol{x}$ を省略して単に y の分布 $p(y)$ と書くことにする．データ D_N を用いた $\boldsymbol{\xi}$ の事後分布は

$$p(\boldsymbol{\xi}|D_N) = \frac{1}{Z(D_N)}\pi(\boldsymbol{\xi})\prod p\left(y_i, \boldsymbol{\xi}\right), \tag{30.32}$$

である．ここで，

$$Z\left(D_N\right) = \int \pi(\boldsymbol{\xi})\prod_{i=1}^{N} p\left(y_i|\boldsymbol{\xi}\right) d\boldsymbol{\xi} \tag{30.33}$$

は D_N の確率であり，(30.32) における正規化定数に相当する．学習後に現れる次のデータ（新しいデータ）を $y_{N+1}, \boldsymbol{x}_{N+1}$ とすれば，

$$Z\left(D_{N+1}\right) = \int \pi(\boldsymbol{\xi})\prod_{i=1}^{N+1} p\left(y_i|\boldsymbol{\xi}\right) d\boldsymbol{\xi} \tag{30.34}$$

を用いて予測分布は

$$p\left(y_{N+1}\,|D_N\right) = \frac{Z\left(D_{N+1}\right)}{Z\left(D_N\right)} \tag{30.35}$$

のように Z を用いて書ける．

Bayes 推論における学習結果の性能は，真の分布 $q(y|\boldsymbol{x})$ と予測分布 $p\left(y\,|\boldsymbol{x}, D_N\right)$ がどのくらい離れているかで評価できる．これが汎化誤差 $l_{\mathrm{gen}}\left(D_N\right) = KL\left[q(y) : p\left(y\,|D_N\right)\right]$ である．これは，データ D_T に依存するから確率変数である．l_{gen} を評価するため，尤度比統計量

$$K_N(\boldsymbol{\xi}) = \frac{1}{N}\sum_{i=1}^{N} \log\frac{q\left(y_i\right)}{p\left(y_i, \boldsymbol{\xi}\right)} \tag{30.36}$$

を使う．これを用いれば，予測分布は

$$p\left(\boldsymbol{\xi}\,|D_N\right) = \frac{\pi(\boldsymbol{\xi})}{Z_0\left(D_N\right)}\exp\left\{-NK_N(\boldsymbol{\xi})\right\} \tag{30.37}$$

のように書ける．ただし，

$$Z_0\left(D_N\right) = \int \exp\left\{-NK_N(\boldsymbol{\xi})\pi(\boldsymbol{\xi})d\boldsymbol{\xi}\right\} \tag{30.38}$$

と置いた．ここで，確率的複雑さと呼ばれる量を $F\left(D_N\right) = -\log Z_0\left(D_N\right)$ で定義する．このとき，汎化誤差は

$$l_{\mathrm{gen}}\left(D_N\right) = -E_{y_{N+1}}\left[\log\frac{Z_0\left(D_{N+1}\right)}{Z_0\left(D_N\right)}\right] \tag{30.39}$$

と書ける．よって，データについて期待値を取れば

$$L_{\mathrm{gen}} = E\left[F\left(D_{N+1}\right) - F\left(D_N\right)\right] \tag{30.40}$$

となる．したがって，こうした量を計算するのには，確率的複雑さ F の期待値

$E[F(D_N)]$ が，N を大きくしたときに漸近的にどう振る舞うかを見ればよい．

正則モデルにあっては，これは簡単で前と同じような漸近展開の手法を用いて，$E[F] \sim p\log N$ となる．したがって，$L_{\rm gen} = p/T$ が言える．しかし，特異モデルにあっては，これが成立しない．

渡辺の理論はこれを計算するもので[8~10]，広中の特異点の解消理論を駆使し，さらに佐藤の代数解析を用いて計算する．ここではとても紹介することはできないが，これがオーダー1の確率変数 R を用いて，$F(D_T) \sim \lambda \log T + R$ と書けることを導いた．λ は有理数である．この λ の計算に，広中の特異点解消定理，佐藤の代数解析を用いるので，代数幾何の高度な理論が必要になってくる．

終わりの一言

連載を始めてから，いつの間にか3年の歳月が流れた．初めは十分に理解可能な，教科書風のものを構想していた．しかし，情報幾何の応用の局面が広がり，さらに国際的にも大きな関心を呼んできたので，数学的なしっかりとした体系と言うよりは，トピックス的な応用に紙数を割くことになった．話題は高度であるので，すべてを納得のいくように書くことはできない．したがって各話題について情報幾何からの見方を紹介するというスタイルになった．一方，連載中でも新しい話題や仕組みが分かってきて，私がそこに夢中になったため，未発表の細部に深入りしてしまった部分もあった．

長年にわたって付き合ってくれた読者に感謝するとともに，これから全体を整理して一冊にまとめ直し，あらためて世に問いたい．

参考文献

1) 福水健次，栗木哲，竹内啓，赤平昌文，『特異モデルの統計学』，岩波統計科学のフロンティア，7, 2004.
2) K. Fukumizu, Likelihood ratio of unidentifiable models and multilayer neural networks, *Annals of Statistics*, **31**, 833–851, 2003.
3) S. Amari, H. Park and T. Ozeki, Singularities Affect Dynamics of Learning in Neuromanifolds, *Neural Computation*, **18**, 1007–1065, 2006.
4) H. Wei, J. Zhang, F. Cousseau, T. Ozeki and S. Amari, Dynamics of Learning Near Singularities in Layered Networks, *Neural Computation*, **20**, 813–843, 2008.
5) F. Cousseau, T. Ozeki and S. Amari, Dynamics of Learning in Multilayer Perceptrons Near Singularities, *IEEE Transactions on Neural Networks*, **19**, 8, 1313–1328, 2008.
6) H. Wei and S. Amari, Dynamics of learning near singularities in radial basis function networks, *Neural Networks*, **21**, 989–1005, 2008.
7) J. Milnor, On the concept of attractor, *Communications of Mathematical Physics*, **99**, 177–195, 1985.
8) 渡辺澄夫，『代数幾何と学習理論』，森北出版，2006.
9) S. Watanabe, Algebraic analysis for nonidentifiable learning machines, *Neural Computation*, **13**, 899–933, 2001.
10) S. Watanabe, Algebraic geometrical methods for hierarchical learning machines, *Neural Networks*, **14**, 1409–1060, 2001.

（あまり・しゅんいち，理化学研究所脳科学総合研究センター）

科学と社会 Science & Society

最終回　国家・学問・戦争の諸相

科学は危機をどう生き延びたか

岡本　拓司

前々回・前回は，第二次大戦下のアメリカ・日本の科学者の動向を検討した．よく知られている通り，第二次大戦の最末期には，科学，特に物理学の現実的な威力と，科学研究における日米間の懸隔を如実に示す出来事が生じ，戦争の帰趨に決定的な影響を及ぼした．その数年後には，しかし，湯川秀樹（1907–1981）が日本人として初めてノーベル賞を受賞し，少なくとも素粒子理論においては日本が世界の先端に位置していたことを明らかにした．本連載の一応の結びとなる今回は，国家・社会と科学の関係がめまぐるしく変化した第二次大戦末期から敗戦後数年までの間に，日本の指導層や科学者がどのように振舞ったかを点描し，戦前から戦後にかけて生じた断絶と連続を指摘することとしたい．

20.1「腹を切る」：原子爆弾投下と仁科芳雄

日本における原子力の軍事利用に関する研究の拠点であった理化学研究所（理研）は，昭和20年（1945年）4月13日夜からの空襲により7割ほどが焼け，大サイクロトロンは無事であったものの，小サイクロトロンなどの他，ウラン235を濃縮するための熱拡散分離塔も被害を受けた．自身の家も焼けた仁科芳雄（1890–1951）は，5月には原子力利用に関する研究の中止を決意した．同年7月，金沢に疎開していた仁科は，研究員に書を求められると「本来空」と認めたが，周囲はその様子を見て，研究もできず家も焼かれて「虚無的」な状態にある彼の心境を想像した[1]．

同年8月6日，広島に原子爆弾が投下された．翌7日の朝，陸軍から訪問者があって仁科に広島で原子爆弾の調査に当たるよう要請し，次いでやってきた同盟通信社の記者が，アメリカが広島に原子爆弾を投下したとの報道があったこと，およびこれについて大統領のトルーマン（Harry S. Truman, 1884–1972）が声明を発したことを伝えた[2]．トルーマン声明は，その冒頭で，16時間前に広島に投下されたのは，TNT火薬2万トン以上に相当する威力を持つ原子爆弾であることを告げていた．さらに，ドイツもその開発を目指したが果たさず，米国が英国の協力の下で多大な費用と資源を傾けて成功に至ったことも記していた．原子爆弾については，以前にもドイツで開発されたなどの報道が現れており，その内容はおおよそ荒唐無稽なものであったが，今回はトルーマン声明の数字が，研究員の玉木英彦（1909–2013）が昭和18年（1943年）に得た値と一致することから，仁科は本物かもしれないと直観した[3]．

仁科は，8月7日の午後，飛行機で広島に発っ

たが故障で引き返し，8日午後に再び出て夕方に広島に到着した．しかし，この間にも広島の惨状に関する情報には接している．

8月7日の夜，仁科が玉木に宛てて書いた手紙[4]が残されており，この時点での彼の心理状況をよく物語っている．手紙の最初の一文は，「今度のトルーマン声明が事実とすれば吾々「ニ」号研究の関係者は文字通り腹を切る時が来たと思ふ」というものであり，切腹の時期は広島から帰ってから話すと続けられている．日本の原子爆弾開発の中心人物が，広島への原子爆弾投下の報に接して最初に考えたのは，責任をとって切腹することであった．具体的な時期も相談すると告げていることから，この覚悟は真剣なものであったと思われる．

仁科が感じていた責任とはどのようなものであったか．まず考えられるのは，大量の資金や資源，人材を費やしておきながら，結局新型爆弾の開発には成功しなかったことに対する責任である．内閣書記官長であった迫水久常（1902–1977）によれば，8月8日の夕刻，仁科が書記官長室を訪ねて，広島に投下されたのが原子爆弾であったことに間違いないと述べ，自分たち科学者が至らなかったことは国家に対して申し訳ないと告げたという[5]．8日の夕刻といえば仁科は広島に着いたばかりであり，本格的な調査は翌日から始まるので，この記述は何らかの記憶違いを含んでいると思われるが，さらに早い時期の回想[6]と比較しながら解釈すると，日本の科学者の中に，自分たちが原子爆弾の開発において敵側に後れをとったことの責任を国家に対して感ずる者があったと迫水が記憶していたことは了解できる．

一方で，しかし，戦局が悪化する中で研究が進まないことに焦慮する，仁科を含む科学者に対し，軍の当事者たちはしばしば，今度の戦争ではなく次に間に合えばよいという旨の発言をしている[7]．開発に成功しなかったこと自体については，依頼者の軍も了承しており，研究者たちに切腹を覚悟させるほどの責任感を生じさせたとは考えにくい．

より深刻であったのは，理研の研究者を含む日本の開発担当者が，今度の戦争に間に合わないのは日本ばかりではなく，敵国側も同様であるという観測を軍や政府に対して告げていたことであったと思われる．理研から発せられたこの見込みの具体例としては，昭和20年6月28日付で熱拡散法の中止を陸軍兵器行政本部に報告した際の文章がある[8]．また，迫水の回想にも，昭和19年（1944年）秋，大倉喜七郎（1882–1963）が，仁科，湯川秀樹，菊池正士（1902–1974），水島三一郎（1899–1983）などを招いて，高松宮宣仁（1905–1987）臨席の下で座談会を開いた際，話は原子爆弾にも及んだが，原理は分かっているものの，「工業的に考えると，いかに米国でも，ここ数年の間にこれを完成するとは思えない」との見解で一致したというものがある[9]．迫水が8月8日に聞いたという仁科の「申し訳ない」という言葉も，真意としては，敵側の状況に対する判断の誤りに関わるものであったのかもしれない．

長岡半太郎（1865–1950）のように，大戦中には原子力の兵器利用は実現しないという観測を公然と表明する者もいた．長岡は，昭和19年1月に開催された海軍科学技術審議会の第一小委員会の中で，核分裂のエネルギー源としての利用は近い将来には実現しないと述べ，八木秀次（1886–1976）も賛成した．アメリカでは4年前から実用研究をしているとの指摘には，長岡は，アメリカでも不可能であると答えた[10]．さらに，昭和19年12月には，核分裂の兵器利用の困難についての見解を論説として公表してもいる[11]．文章全体からは，長岡は当時は連鎖反応などに理解が及んでいなかったのではないかとの印象を受けるが，論説末尾の「付記」には，「記者は目下先きの見透しのついた兵器研究に没頭し時を稼がねばなりませぬから，この愚論につき面談若しくは書状で質問せらるゝことは失礼ながら謝絶致します」とあり，核分裂の利用が荒唐無稽な想像にすぎないと判断されていたことが分かる．

日本の科学者は，核分裂の爆弾としての利用や，ウラン235の濃縮について，ほとんど見込みも立てられない状態であり，自分たちのこうした状況をもとに，アメリカでも数年内の実用化は不可能

であると判断していた．つまり，彼らの判断は，アメリカの科学技術に関する見積もりの誤りというよりは，現象そのものについての理解の不足に由来しており，それは，彼らの科学者としての——能力とは言わないまでも——到達度の低さを意味していた．ただし，アメリカが開発に成功した原子爆弾が日本に投下されたという事実が如実に示した彼らの判断の誤り——科学者としての至らなさ——についてどう感じたかは，世代や立場，或いは性格によって異なる．開発の当事者であった仁科が切腹も覚悟したのに対し，誤った判断を公刊してさえいた長岡が，その責任を深刻に受け止めた形跡はないようである．

20.2 研究者の「人格」

仁科の8月7日の手紙の次の段落には，トルーマン声明が原子爆弾の誕生を米英の科学者の努力の勝利と称えていることを受けてか，「要するにこれが事実とすればトルーマンの声明する通り，米英の研究者は日本の研究者即ち理研の49号館の研究者に対して大勝利を得たのである」と記されている．次いでこの事実に対する仁科の解釈が述べられており，それは，「これは結局に於て米英の研究者の人格が49号館の研究者の人格を凌駕してゐるといふことに尽きる」というものであった．

原子爆弾開発の成功を勝利と称える点では，仁科はトルーマン声明に倣っているが，これに加えて，その勝利は開発に携わった研究者の「人格」が優れていることを示すという判断がなされている．原子爆弾を誕生させた研究者の人格が優れていると主張しているかのように思われるこの文章は，いったい何を意味しているのであろうか．

仁科が昭和15年（1940年）に発表した文章には，研究者の人格が研究成果を左右すると述べた箇所を持つものがあり，上述の「人格」もそれに準じて理解することができる．この文章は，アメリカの科学についての概説であり[12]，仁科は末尾で，大サイクロトロンの建設に関して，材料の確保の斡旋や青写真の送付など，援助を惜しみなくあたえたローレンス（Ernest Orlando Lawrence, 1901–1958）について触れ，「科学の発展は只手や頭の先きの技術の問題ではなく，これに携はる人の人格の如何による事である」と記した．

同様の表現は，サイクロトロン建設に関する知識を得るためにローレンスの下に滞在していた理研の矢崎為一（1902–1970）の文章の中にもある．矢崎は，昭和12年（1937年）の理研原子核実験室を紹介した文章[13]の中で，この年に理研を訪れたボーア（Niels Henrik David Bohr, 1885–1962）に言及し，ボーアが，学問上の議論以外にも，「其人格を以て物理学者が如何に行き又研究すべきかを如実に示された」と記した．矢崎はこのとき，ローレンスが，「君が偉大な物理学者にならうとしたら先づよい人間になり給へ」と言っていたことを思い出し，ボーアこそそのような人物であると実感した．「かゝる人によつてはじめて立派な物理学上の貢献がなされるのは当然の事と思ふ」というのが，ボーアに接しての矢崎の感慨であった．

仁科の周辺では，ローレンスやボーアを念頭において，科学者の得る成果は人格の賜物であると言われていたようである．原子爆弾投下の報に接して，自身の責任の問題に次いで仁科が思い至ったのは，自分たちが開発の手掛かりさえ得ることのできなかった原子爆弾を完成させた英米の研究者たちは，その成果から評価する限り，自分たちを人格において凌駕しているという評価であった．

日米開戦後まもない頃に仁科が確認したのは，科学者には，戦時下でも純粋科学の研究に邁進する必要があるという決意であった．日米開戦前の世界の物理学者の主要な関心の一つは湯川の中間子論の成否であり，仁科は，日本の物理学者として，この課題の解決に関して他国の研究者の後塵を拝するわけにはいかず，戦時下でも研究は中断できなかった．

原子爆弾の開発は「純粋科学」の課題ではない．しかし，戦時下で，勝利を目指す各国の要請に従って，日米欧の物理学者の多くが原子爆弾の開発に携わることとなった．仁科は，開戦前からアメリカで核分裂の兵器利用が研究されていることを知っ

ていたが，広島からの情報やトルーマン声明により，各国の物理学者が互いの状況を詳細には知らないまま参加していた原子爆弾開発の競争に，ドイツや日本を引き離して英米の物理学者たちが勝利したことを理解した．原子爆弾の完成を研究成果として評価した仁科は，それに成功した研究者の人格を賞賛したのである．仁科や矢崎も想像していたと思われるが[14)]，仁科の師であり矢崎が人格者と称えたボーアは，英米での原子爆弾開発の初期には重要な役割を果たしており，ローレンスは計画全体の最重要人物の一人であった．

20.3 原子爆弾投下と講和への動き

原子爆弾の投下は，日本全体の行く末にも大きな影響を及ぼしており，これ以降，ポツダム宣言受諾による終戦への動きが表面化していった．8月9日に技術院に出向いた長岡は，この時点でも，広島に投下されたのが原子爆弾であるとの観測を疑い，「原子に悪因縁を付けて自体を変じ」ようという政治家の動向を感じとっていた．原子爆弾は，たしかに，「和平工策でもやるには国民を威嚇するに此上も無き好材料」であることには間違いないと判断した上で，前年の自身の核分裂の兵器利用の可能性についての見通しを振り返ることもなく，周章狼狽する政府の様子を，「事態は維新の際幕府の内部に感ぜられたものと大差なからう」，「八十余年の怪夢は覚めて再び暗に還る」と描写している．維新前後の騒動を，伝聞によるとはいえ身近なものとして知る長岡は，原爆投下後の混乱にも大きくは動じていなかったようである[15)]．

実際には，戦局の悪化が顕著になる頃から，政府・軍の中に講和への動きは生じていたが，原子爆弾の投下がこれを急激に加速した．8月7日には，昭和天皇（1901–1989）は内大臣の木戸幸一（1889–1977）から広島の状況について情報を得始めており，8日にはソ連の仲介による終戦の実施を政府に求めた[16)]．同日にはソ連が日ソ中立条約を破って満洲国に侵攻しており，9日にはこれを受けてポツダム宣言受諾について検討するため最高戦争指導会議構成員会議が開かれたが，会議中には長崎への原子爆弾投下があった．これで即時に講和が実現してもよいように思われるが，実際には，よく知られている通り，ポツダム宣言の受諾が決定したのは14日深夜であり，国民に対するラジオ放送での発表は15日正午となった．原子爆弾の投下が講和への動きを加速させたことは間違いないが，その具体的な過程については検討する余地がある．

第二次大戦の中盤までは，日本側はドイツの快進撃に期待するところが大きかったが，スターリングラートでドイツが大敗を喫し，日本もガダルカナルから撤退を余儀なくされた昭和18年には，陸軍においても講和への道筋が想定されるようになっていた[17)]．翌年にドイツの敗色がさらに濃くなると，昭和天皇も，9月には，ドイツ降伏を機に，武装解除や戦争責任追及を伴わない，無条件降伏（カイロ宣言（1943年11月）で連合国が目標に掲げていた）ではない形での講和を考えるようになった[18)]．

戦争の開始にも目的はあるが，その終結にも目標はあり，敗退しつつある国家にとっては，必然的に，何かを得ようというよりは，何を守れるかが問題となる．守る対象とは，戦争が直接関わるものばかりではなく，例えば国際的な信義も重要であり，日本としては，日独伊単独不講和協定（1941年締結）がある限りは，ドイツ降伏（1945年5月8日）以前に単独講和に臨むことはできなかった．ドイツの状況はこの点でも日本の選択に影響していた．

ドイツ降伏後には，しかし，日本には守るべきものは多くは残されていなかった．昭和天皇は，昭和20年5月には天皇家の存続のみを条件とする終戦を想定するようになった[19)]．これでも連合国が公表した目標である無条件降伏とは異なる以上，わずかな条件でも勝ち取る目算はあったと考えなければならない．その目算によっては，得られると見込まれる条件は，昭和天皇個人の意思とは別に，天皇を主権者とする統治形態の維持（国体護持）にまで膨らむこととなった．

条件つきの降伏を得るための手段は，大きく分けて２つあった．一つはソ連を介した和平交渉である．交渉の進展には，戦時の社会主義的な統制経済は，英米の民主主義よりもソ連に近いとする発想も影響していた[20]．これに対して，近衛文麿（1891–1945）のように，戦局の悪化が赤色革命を起こすことを警戒する者もあったが，ソ連は，参戦に踏み切るまでは，講和を仲介し得るほぼ唯一の中立の大国であったために，同国への働きかけはその満洲侵攻の当日まで続けられた．８月８日のソ連参戦は，結果的に，その努力を無意味なものとし，条件つき降伏を獲得する手段の一つを無効にした．同時に，敵側にソ連が加われば勝算はないと見込んでいた陸軍の継戦の意欲を大いに殺ぐこととともなった[21]．

ソ連参戦は，条件つき降伏を勝ち取るためのもう一つの手段の成否にも影響を及ぼしたが，しかし，８月９日以降も，この手段への期待は完全に損なわれたわけではなかった．もう一つの手段とは本土決戦である．海軍の主導で南洋の島々で孤立し，悲惨な結末を迎えるという戦いを余儀なくされていた陸軍には，大部隊を駆使しての戦闘が可能になるとして，本土における最後の決戦に期待する者も多かった[22]．国民の多くを戦闘に直接用いる準備も，国民義勇隊の結成（昭和 20 年３月），義勇兵役法の制定（同６月公布）によって進んでいた[23]．後者によって組織される民兵組織，国民義勇戦闘隊が使うことが想定されていた武器には，弓や竹やりさえ含まれていたが，勝敗を度外視すれば戦えないわけではない．

勝敗を度外視するかどうかは，終戦によって何が守れるかに依存していた．陸軍の井田正孝（1912–2004）のように，本土決戦によって現実の天皇や三種の神器が滅びても，日本の国体が理念として永遠に残れば戦う意味はあると考えれば[24]，徹底抗戦した末の全滅さえ選択肢のうちに含まれることになる．天皇個人の安否についてももはや保証はなく，昭和天皇自身は，昭和 20 年７月末には，本土決戦にあたっては三種の神器を守って運命をともにする覚悟を固めていた[25]．

原子爆弾の投下は，しかし，本土決戦についての想定に変化をもたらすこととなった．特に昭和天皇の言動は，その変化を明瞭に反映している．７月末本土決戦を覚悟していた昭和天皇は，広島への原子爆弾投下後には，既述の通り政府に講和を指示した．おそらくは，原子爆弾の用いられる本土決戦は，三種の神器と自身の滅亡を超える何事かをもたらすと直感したのであり，その何事かとは，戦後に昭和天皇が皇太子に書き送った手紙から想定すると，「国民の種」[26]が残らなくなる事態，すなわち民族の滅亡であったと思われる．

ヒトラー（Adolf Hitler, 1889–1945）が自殺するまでに追い詰められてようやく終結したドイツの戦いでも，ドイツ国民が滅亡することはなかった．ドイツ降伏後に，ソ連を加えた連合国が総力を挙げて日本に向かい，国民義勇戦闘隊までもがこれに立ち向かったとしても，「国民の種」が絶えるとは昭和天皇も想定はしなかったであろう．実際，ソ連は，少なくとも表向きは，ドイツ国民が戦争の最終局面で経験した危険や破壊から日本国民を救うことを目的に参戦していた[27]．

原子爆弾の威力について知ったあとの昭和天皇は，しかし，この兵器が本土決戦で用いられれば，国民の滅亡という事態が生じかねないと考えたものと思われる．昭和 20 年７月 26 日に発表されたポツダム宣言は，ドイツ国民が経験した破壊力を遥かに超えるものが日本に向っており，それは日本国本土の完全な破壊をもたらすと告げていた[28]．昭和天皇のみならず，この宣言に接した者は，原子爆弾投下後，注意深くさえあれば，その文言が誇張ではないことに気づいたであろう．

20.4 国体と国民

ソ連参戦で英米との直接交渉以外の道はなくなり，原子爆弾の登場で本土決戦が国民の滅亡の危機を意味するようになれば，講和以外の選択はあり得なくなったようにも思われる．陸軍関係者も含む多くの人々がそう了解したとは思われるが，陸軍の一部には継戦を主張する者がおり，陸軍大

臣や参謀総長も彼らに押し切られたまま閣議や御前会議に望まなければならなかった．

継戦派のよりどころは，ポツダム宣言受諾は国体護持を保証しないという指摘である．8月10日には，天皇の統治の大権に変更を及ぼさないことを条件としてポツダム宣言を受諾する旨トルーマン大統領に申し入れがなされたが，12日に発せられた連合国回答文は，国体護持を明確には保証していなかった[29]．守るべきものが守られないのであれば，たとえ国民が滅亡しても飽くまでも戦うというのが継戦派の主張であり，極めて論理的である——ただし，論理的であることはときに空しくもあるとも思わせる．実際は何を目的としてのことかは不明ながら，何とか本土決戦に持ち込みたいというのが本心ではなかったかと思われる．

実際にそう信じていたかどうかは明らかではないが，陸軍側は原子爆弾についても軽視する姿勢を示した．広島への投下後は，あれが最後の一発であったという可能性を示唆して抵抗し[30]，長崎への投下でその可能性が否定された後は，原子爆弾の正体を知るはずもない米空軍将校に8日から暴行を加え続けて無理やり得た情報をもとに，爆弾は電気仕掛けで対策はあると主張するようになった[31]．荒唐無稽ではあるが，アメリカも原子爆弾をこれ以上はもっていなかった．また，アメリカは，硫黄島の戦いで日米の損害比が初めて逆転したことや，1カ月で終結すると見込まれた沖縄戦が3カ月に及ぶ難戦となったことに衝撃を受けていた[32]．もはや形勢の逆転はないものの，徹底抗戦で敵をまだ苦しめうるという陸軍の想定は全くの見当違いであったわけではない．

国体護持が目標である限りは，継戦派の主張の論理的な正しさは揺るがず，また軍事の専門家集団の主張にはそれなりの根拠もあった．単にもはや勝機はないというのみでは，国体護持を目的とする国家が，その保証のないまま戦争を終わらせることはできない．この窮地で生じたのは，徐々に目標そのものを変化させることであった．

あまり多くはないものの，昭和天皇の原爆投下から終戦に至るまでの発言を見ると，彼が，国体護持——昭和天皇自身にとってはそれが単に天皇家の存続を意味していた可能性も高いが——は叶うと説得しながら，同時に，国体護持に代わる事項を徐々に守るべきものとして主張していったことが分かる．即ち，昭和天皇は，8月10日午前0時からの御前会議の最後では，国民を苦しめ文化を破壊し世界人類の不幸を招くことを欲しないと述べており，14日午前の午前会議では，国土も民族も国体も破滅する事態を避けたいと主張した[33]．国体護持が目標であれば，それが保証されない限り国民は最後の一人まで戦うほかはないが，達成すべき目標は，次第に，国民を滅亡から救うことを含むようになっていき，原子爆弾の使用されかねない本土決戦を選択肢から外すのが自然であると感じられるような論理が築かれていった．それ以前は，国民は国体護持のためのいわば「手段」であったが，次第に，国民を全滅から救うことが，国家がとるべき選択の「目標」となっていった．

国家が守るべきものを国体から国民へと転換させることができる立場に居たのは，昭和天皇ただ一人であった．天皇以外の国民は国体を守るべき責務を負わされていたのであり，国体を捨てて国民を守るべきであると主張することはできなかった．

国民の滅亡を避けるために講和を選ぶという主張は，「終戦の詔書」ではより明確に表現され，国民が国家の守るべき最高の価値であるという理念は，戦後は日本国憲法の定めるところとなった．しかしそれ以前に，国体から国民への価値の転換は生じていた．昭和天皇が，おそらく無意識のうちに，原子爆弾が使用される本土決戦という悪夢に戦慄しながらこれに着手したのであった．

20.5 科学の価値

昭和20年8月15日に，原子爆弾の調査を終えて理研に戻った仁科が最初に気にかけたのは，サイクロトロンの真空の漏れであったようである．切腹を覚悟した緊張感は消え去っていた．何事もなかったかのように純粋科学の世界に戻った仁科の君子豹変ぶりは，すでに原子爆弾の調査の中で

も予想されていた[34]．原子爆弾の投下から終戦に至る過程で，軍の勢いは急激に弱まり，同時に仁科が感じていた責任も消滅したのであろう．

敗戦後，社会全体の価値観の転換は大きく進んだ．昭和21年5月の食糧メーデーでは，「詔書　国体はゴジされたぞ　朕はタラフク食ってるぞ　ナンジ人民　飢えて死ね」と記したプラカードが掲げられ（「プラカード事件」）[35]，国体から国民への価値の転換が，その実現に最初に関わった昭和天皇を揶揄する文言によって鮮やかに表現された．純粋科学の世界に戻っていた仁科も，戦後は「人民のために人民が行ふ政体」がとられるようになったことに気づき，今度は，「人民各自の人格の高低はとりも直さず，わが国の浮沈を決定するものに他ならない」と考えるようになった[36]．

国家と社会の変動の中で，日本の科学への評価も変化する可能性はあった．戦時中，新兵器への期待を抱かせ，多くの資源や人材を使いながら，日本の科学者たちは結局戦争に対して大きな貢献を行うことはできず，核分裂の兵器利用に関する彼らの見込みも外れた．原子爆弾の投下の後，ポツダム宣言受諾が決意される局面では，鈴木貞一（1888–1989）のように，この戦争に負けたのは日本の軍ではなく，科学技術であると理解することで，軍の名誉は保たれると理解する者もいた[37]．

日本の科学者たちは，しかし，「科学戦」に敗れた責任を問われて萎縮するどころか，むしろ新たな時代を先導する知性としての期待を集めるようになった．戦後には，戦時中，軍人や政治家が科学者の主張に充分耳を傾けなかった，科学戦に敗れたのであるから科学振興に邁進すべきであるという主張から，さらに進んで，社会に科学的な精神がいきわたっていれば無謀な戦争への道は歩まなかったという指摘も現れた[38]．政治の領域で特に若い世代の支持を集めた共産党の科学技術部は，昭和21年の『前衛』に「日本の科学・技術の欠陥と共産主義者の任務」[39]と題する論説を発表し，封建的支配機構を一掃するために科学者が果たすべき役割を示した．また，占領下の日本で大学や研究所を回って科学研究の実態を調査したアメリカの科学者たちは，日本の同僚たちが，困窮する社会の要請に応えることよりも，自分たちの仕事の文化的価値を重視している点に驚いている[40]．左右両翼，新旧世代にわたって，科学の価値は信奉され続けていた．

仁科が気にかけた中間子論の成否は，昭和22年（1947年）に宇宙線中に中間子が発見されたことによって確認され，戦時中から戦後にかけて日米両国で提唱された二中間子論が正しかったことが明らかになった．これにより，昭和24年（1949年）には，湯川が日本人初のノーベル賞を受賞することとなった．くりこみ理論に至る朝永振一郎（1906–1979）の研究も欧米の関心を集めており，東京の焼け跡から送られる彼の研究は，のちに「深海からの声」（“a voice out of the deep”）と評された[41]．戦時下でも純粋科学の研究を継続すべきであると主張した仁科のような人々によって，国家が競いあう場とは別に，独自の連続性をもつ科学の世界が支えられており，その世界に日本は一定の地歩を占め始めていたのである．

日本の科学は，戦前戦後の断絶を超えて，単に連続性を保ったのみならず，戦前戦中の蓄積を基礎に戦後にはさらに大きく成長していった．また，国外に目を転ずると，同様の傾向は，軍事面においてより顕著であった．原子爆弾の登場後は，これの保有・非保有が一国の発言権を大きく左右するようになり，さらには科学研究は国防に直結すると理解され，国家から相応の支援と指示を受けることとなった．

その反面，核をもつ大国同士が直接的な戦闘状態に入ることは困難になった．従来は戦争遂行の手段とみなされていた科学が，想像を越える破壊力を実現させたために，国際関係の基本的条件が変化せざるを得なくなった．第一次大戦後21年で次の大戦が勃発したのとは対照的に，第二次大戦後，世界規模での戦争は起こっていない．

これらは，もちろん戦後の科学の展開の一側面に関わるものにすぎない．戦後の科学の姿を描くためには，また別の機会が必要となろう．しかし最後に一点，戦後に科学が論じられる際には，そ

の成果が称えられるばかりではなくなったという事実には触れておいてもよいかもしれない．

日本における国体から国民への価値の転換は，わずか１発ずつの爆弾の瞬時の爆発が広島と長崎にもたらした，かつてない規模の被害と引き換えに生じていた．戦後，科学について，何であれ世界規模・人類史規模の枠で語ろうとすれば，広島と長崎の経験を無視することはできなくなった．これにより，科学に関する議論全般は，従来にはなかった陰影を帯びることとなった．

20回にわたって，明治維新前後から20世紀半ばまでの科学の歴史について議論させていただいた．20回かけても充分な検討ができたとは思われないが，今回はここまでで一応の終点とし，考察をさらに深める機会はまた別に求めることとしたい．連載中は多くの方々のお世話になった．この場をお借りして深く感謝申し上げる．

参考文献

1) 朝永振一郎・玉木英彦編『仁科芳雄　伝記と回想』（みすず書房，1952年），195ページ．
2) 仁科芳雄，「原子爆弾」，『世界』，**3**号，1946年3月，108–122ページ．
3) 山崎正勝，『日本の核開発：1939～1955——原爆から原子力へ』，績文堂出版，2011年，68ページ．
4) 中根良平・仁科雄一郎・仁科浩二郎・矢崎裕二・江沢洋編，『仁科芳雄往復書簡集　III』（みすず書房，2007年），1142–1143ページ．
5) 迫水久常，『機関銃下の首相官邸』（ちくま学芸文庫，2011年），265ページ．原著は恒文社刊，1964年．
6) 迫水久常，「終戦の真相」，『正論』，**375**号，2003年9月，48–67ページ．
7) 山崎，前掲[3]，『日本の核開発』，63ページ．
8) 山崎，前掲[3]，『日本の核開発』，70ページ．
9) 迫水，前掲[5]，『機関銃下の首相官邸』，262ページ．
10) 山崎，前掲[3]，『日本の核開発』，24–25ページ．
11) 長岡半太郎，「原子核分裂を兵器に利用する批判」，『軍事と技術』，1944年12月，1–6ページ．
12) 仁科芳雄，「アメリカの科学」，『理想』，14年6冊，1940年6月，655–666ページ．
13) 矢崎為一，「研究室概観　理化学研究所原子核実験室」，『科学』，**7**巻**7**号，1937年6月，292–295ページ．
14) 仁科芳雄，『仁科芳雄博士遺稿集　原子力と私』（補訂版，学風書院，1951年），130ページ．
15) 板倉聖宣・木村東作・八木江里，『長岡半太郎伝』（朝日新聞社，1973年），676–677ページ．
16) 古川隆久，『ポツダム宣言と軍国日本』（吉川弘文館，2012年），148ページ．
17) 山本智之，『主戦か講和か　帝国陸軍の秘密終戦工作』（新潮社，2013年），65–68ページ．
18) 古川隆久，『昭和天皇』（中公新書，2011年），290ページ．
19) 古川，前掲[16]，『ポツダム宣言と軍国日本』，141ページ．
20) 鈴木多聞，『「終戦」の政治史　1943–1945』（東京大学出版会，2011年），115ページ．
21) 鈴木，前掲[20]，『「終戦」の政治史』，165ページ．
22) 山本，前掲[17]，『主戦か講和か』，163–166ページ．
23) 吉田裕，『アジア・太平洋戦争』（岩波新書，2007年），211–212ページ．
24) 鈴木，前掲[20]，『「終戦」の政治史』，112ページ．
25) 木戸日記研究会校訂，『木戸幸一日記　下巻』（東京大学出版会，1966年），1220–1221ページ．
26) 高橋紘，『象徴天皇』（岩波新書，1987年），3ページ．
27) 古川，前掲[16]，『ポツダム宣言と軍国日本』，148ページ．
28) 迫水，前掲[6]，『機関銃下の首相官邸』，242ページ．
29) 鈴木，前掲[20]，『「終戦」の政治史』，175–177ページ．
30) 五百旗頭真，『日米戦争と戦後日本』（講談社学術文庫，2005年），152–153ページ．
31) 鈴木，前掲[20]，『「終戦」の政治史』，160–161ページ．
32) 五百旗頭，前掲[30]，『日米戦争と戦後日本』，101–103ページ．
33) 鈴木，前掲[20]，『「終戦」の政治史』，171・184ページ．
34) 朝永・玉木編，前掲[1]，『仁科芳雄』，194–196ページ．
35) 雨宮昭一，『占領と改革』（岩波新書，2008年），121ページ．
36) 仁科芳雄，「国民の人格向上と科学技術」，『自然』，**1**巻，1946年12月，1ページ．
37) 迫水，前掲[5]，『機関銃下の首相官邸』，264ページ．
38) 中山茂・後藤邦夫・吉岡斉編，『〔通史〕日本の科学技術　1』（学陽書房，1995年）．
39) 武谷三男，『武谷三男著作集　4』（勁草書房，1969年），211–225ページ．
40) Scientific Advisory Group, “Reorganization of Science and Technology in Japan: Report of the Scientific Advisory Group to the National Academy of Sciences, United States of America, Tokyo, Japan, August 28, 1947”（『日本現代教育基本文献叢書　戦後教育改革構想　I期　5』（日本図書センター，2000年）所収）．
41) Makinosuke Matsui and Hiroshi Ezawa, eds., *Sin-itiro Tomonaga: Life of a Japanese Physicist* (Tokyo: MYU, 1995), p.169.

（おかもと・たくじ，東京大学大学院総合文化研究科）

例題形式で探求する 微積分学の基本定理
関数の性質から幾何構造を探る
第9回

面積分(1)

森田　茂之

前回と前々回で述べた曲面の面積の定義を基に，今回から**面積分**を扱うことにする．

9.1 面積分の定義

S を $\mathbb{R}^3$ 内のコンパクトで滑らかな曲面で，境界を持っていてもよいものとする．S 上の実数値関数

$$f : S \to \mathbb{R}$$

が与えられたとしよう．このとき S を面積をもつ有限個の小区域 σ_i に分割し，各 σ_i 上の点 P_i を選べば，和

$$\sum_i f(\mathrm{P}_i) \mathrm{Area}\, \sigma_i$$

が定まる（図 9.1 参照）．もし，極限値

$$\lim_{|\sigma_i| \to 0} \sum_i f(\mathrm{P}_i) \mathrm{Area}\, \sigma_i$$

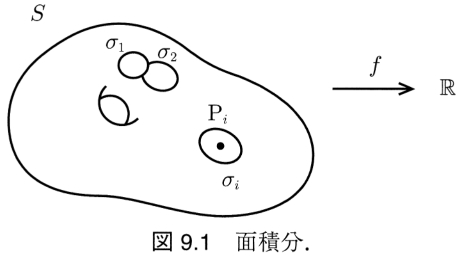


図 9.1　面積分．

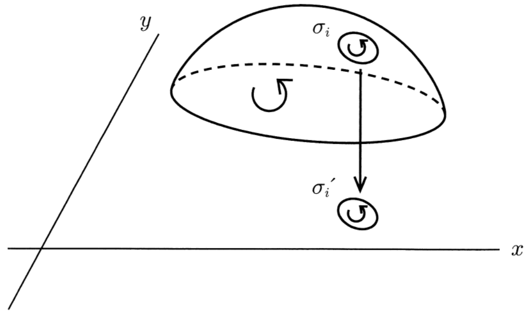


図 9.2　向き付けられた曲面.

が存在し，それが点 P_i の取り方によらず一定であるとき，f は S 上積分可能であるという．ここで $|\sigma_i|$ は σ_i の直径，すなわち σ_i 上の 2 点間の距離の最大値を表す．もし f が連続ならば，それは積分可能であることが知られている．そこで

$$\int_S f d\sigma = \text{上記の極限値}$$

とおき，これを f の S 上の面積分という．とくに値 1 をもつ恒等関数の S 上の面積分は S の面積に等しい．すなわち

$$\int_S 1\, d\sigma = \mathrm{Area}\, S$$

である．

次に曲面 S は向き付け可能とし，一つ向きを指定しておく．S の小区域 σ_i による分割に対し，各 σ_i の xy 平面への正射影の像を σ_i' とする．このとき，上記の面積分の定義において $\mathrm{Area}\,\sigma_i$ を $\mathrm{Area}\,\sigma_i'$ に替えたもの

$$\iint_S f dx dy = \lim_{|\sigma_i|\to 0} \sum_i f(\mathrm{P}_i)\mathrm{Area}\,\sigma_i'$$

が考えられる．これを曲面 S 上の関数 f の xy 方向の面積分という．ただし σ_i' の面積 $\mathrm{Area}\,\sigma_i'$ は "符号付きの面積" とする．すなわち，σ_i の与えられた向きが誘導する σ_i' の向きが，xy 平面の通常の正の向き（時計と反対回りの向き）と一致する場合は正の値を取らせ，逆の向きになる場合（"裏返し" になる場合）は負の値を取らせるものとする（図 9.2 参照）．

これは次のように言い替えることができる．各点 $\mathrm{P} \in S$ において正の向きに長さ 1 の法線ベクトルをたて，それを $\boldsymbol{n}_\mathrm{P}$ とする．そして

$$\boldsymbol{n}_\mathrm{P} \text{ と } x, y, z \text{ 軸の正の方向とのなす角度をそれぞれ } \alpha, \beta, \gamma$$

とする．このとき

$$\boldsymbol{n}_\mathrm{P} = (\cos\alpha, \cos\beta, \cos\gamma)$$

となる．さて上記で小区域 σ 上に点 P を取れば，符号付きの面積 $\mathrm{Area}\,\sigma'$ は

$\mathrm{Area}\,\sigma\cos\gamma$ で近似できる．このことから，xy 方向の面積分は，初めに定義した面積分により

$$\iint_S f\,dxdy = \int_S f\cos\gamma\,d\sigma$$

と表すことができることが分かる．同様にして，yz 方向の面積分および zx 方向の面積分も考えることができるが，それらは

$$\iint_S f\,dydz = \int_S f\cos\alpha\,d\sigma,$$
$$\iint_S f\,dzdx = \int_S f\cos\beta\,d\sigma$$

と表すことができる．

例題 9.1（半球面の重心） $\mathbb{R}^3$ の原点を中心とする半径 r の球面の北半球の部分

$$S_+ = \{(x,y,z)\in\mathbb{R}^3; x^2+y^2+z^2=r^2, z\geq 0\}$$

の重心の座標を求めよ．

解答 S_+ の重心の座標は，明らかな対称性から $(0,0,z_S)$ の形をしている．そして z_S は

$$z_S = \frac{1}{\mathrm{Area}\,S_+}\int_{S_+} z\,d\sigma = \frac{1}{2\pi r^2}\int_{S_+} z\,d\sigma$$

で与えられる．この面積分を求めるために北半球の局所座標として (x,y) を使おう．このとき S_+ 上では $z=\sqrt{r^2-x^2-y^2}$ であるから，前回の記号を使って接ベクトルは

$$\boldsymbol{t}_x = \left(1, 0, -x(r^2-x^2-y^2)^{-\frac{1}{2}}\right),$$
$$\boldsymbol{t}_y = \left(0, 1, -y(r^2-x^2-y^2)^{-\frac{1}{2}}\right)$$

となる．したがって

$$E = (\boldsymbol{t}_x,\boldsymbol{t}_x) = 1 + x^2(r^2-x^2-y^2)^{-1},$$
$$F = (\boldsymbol{t}_x,\boldsymbol{t}_y) = xy(r^2-x^2-y^2)^{-1},$$
$$G = (\boldsymbol{t}_y,\boldsymbol{t}_y) = 1 + y^2(r^2-x^2-y^2)^{-1}$$

から

$$\sqrt{EG-F^2} = \sqrt{1+x^2(r^2-x^2-y^2)^{-1}+y^2(r^2-x^2-y^2)^{-1}}$$
$$= r(r^2-x^2-y^2)^{-\frac{1}{2}}$$

となる．ここで前回述べた局所座標による曲面積の公式 8.2 を使うと

$$\int_{S_+} z\,d\sigma = \iint_{D_r}\sqrt{r^2-x^2-y^2}\,\sqrt{EG-F^2}\,dxdy$$

$$= r \iint_{D_r} dxdy = \pi r^3$$

となる．ただし D_r は $\mathbb{R}^2$ の原点を中心とする半径 r の円板を表す．以上から $z_S = \frac{1}{2} r$ となり，したがって半球面 S_+ の重心の座標は

$$\left(0, 0, \frac{1}{2} r\right)$$

であることが分かった．

比較のために，半球体の重心も求めてみよう．

例題 9.2（**半球体の重心**）　$\mathbb{R}^3$ の原点を中心とする半径 r の球体の赤道面より北の部分

$$D_+ = \{(x, y, z) \in \mathbb{R}^3; x^2 + y^2 + z^2 \leq r^2, z \geq 0\}$$

の重心の座標を求めよ．

解答　D_+ の重心の座標も，明らかな対称性から $(0, 0, z_D)$ の形をしている．そして z_D は

$$z_D = \frac{1}{\mathrm{Vol}\, D_+} \iiint_{D_+} z\, dxdydz = \frac{3}{2\pi r^3} \iiint_{D_+} z\, dxdydz$$

で与えられる．この 3 重積分を計算しよう．

$$\begin{aligned}
\iiint_{D_+} z\, dxdydz &= \int_{-r}^{r} dx \int_{-\sqrt{r^2-x^2}}^{\sqrt{r^2-x^2}} dy \int_0^{\sqrt{r^2-x^2-y^2}} zdz \\
&= \int_{-r}^{r} dx \int_{-\sqrt{r^2-x^2}}^{\sqrt{r^2-x^2}} dy \left[\frac{1}{2} z^2\right]_0^{\sqrt{r^2-x^2-y^2}} \\
&= \frac{1}{2} \int_{-r}^{r} dx \int_{-\sqrt{r^2-x^2}}^{\sqrt{r^2-x^2}} (r^2 - x^2 - y^2) dy \\
&= \frac{1}{2} \int_{-r}^{r} dx \left[(r^2 - x^2)y - \frac{1}{3} y^3\right]_{-\sqrt{r^2-x^2}}^{\sqrt{r^2-x^2}} \\
&= \frac{2}{3} \int_{-r}^{r} (r^2 - x^2)^{\frac{3}{2}} dx \\
&= \frac{2}{3} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} r^4 \cos^4 \theta\, d\theta \quad (x = r \sin \theta) \\
&= \frac{4}{3} r^4 \int_0^{\frac{\pi}{2}} \sin^4 \theta\, d\theta = \frac{1}{4} \pi r^4
\end{aligned}$$

となる．ここで $\int_0^{\frac{\pi}{2}} \sin^4 \theta\, d\theta = \frac{3}{16}\pi$ を使った．以上から $z_D = \frac{3}{8} r$ となり，したがって半球体 D_+ の重心の座標は

$$\left(0, 0, \frac{3}{8} r\right)$$

である．

9.2 面積分と体積

この節では面積分と体積の間にある密接な関係を考える．まず，以前に述べた面積に関するギュルダンの法則の体積に関する類似を述べる．

例題 9.3（体積に関するギュルダンの法則） xy 平面上の $y \geq 0$ の部分にある単純閉曲線を C とし，それが囲む区域を D とする．xyz 空間において，D を x 軸の回りに一回転して得られる立体を V とする．このとき，D の重心の座標を (x_0, y_0) とすれば

$$\mathrm{Vol}\, V = 2\pi y_0 \,\mathrm{Area}\, D$$

となる．すなわち

$$\text{回転体の体積} = \text{子午線面の重心が描く円周の長さ} \times \text{子午線面の面積}$$

となる．これを体積に関するギュルダンの法則という．C が図 9.3 の状況の場合にこの法則を証明せよ．

解答 重心の y 座標は

$$y_0 = \frac{1}{\mathrm{Area}\, D} \iint_D y dx dy$$

で与えられる．したがって

$$\begin{aligned}
2\pi y_0 \,\mathrm{Area}\, D &= 2\pi \iint_D y dx dy \\
&= 2\pi \int_a^b dx \left[\frac{1}{2} y^2 \right]_{\varphi_-(x)}^{\varphi_+(x)} \\
&= \int_a^b \left\{ \pi \varphi_+^2(x) - \pi \varphi_-^2(x) \right\} dx \\
&= \mathrm{Vol}\, V
\end{aligned}$$

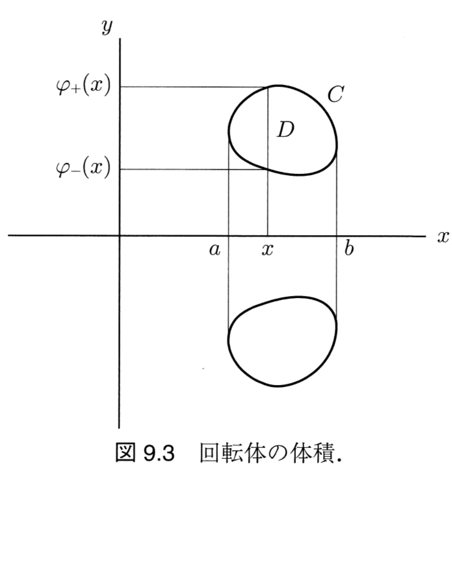


図 9.3　回転体の体積．

となり，証明が終わる．

例題 9.4　$\mathbb{R}^3$ の原点を中心とする半径 R の球面

$$S_R = \{(x,y,z) \in \mathbb{R}^3; x^2+y^2+z^2=R^2\}$$

を考え，外向きに法線ベクトルが出るように向きを付けておくことにする．このとき面積分

$$\int_{S_R} z\,dxdy$$

の値を求めよ．

解答　S_R の北半球，南半球をそれぞれ S_+, S_- と書くことにすれば

$$\int_{S_R} z\,dxdy = \int_{S_+} z\,dxdy + \int_{S_-} z\,dxdy$$

となる．第一項の積分は例題 9.1 の記号で

$$\int_{S_+} zdxdy = \iint_{D_R} \sqrt{R^2-x^2-y^2}\,dxdy$$

となる（ただし極座標を使う関係で半径を R としている）．ここで右辺を極座標に変数変換して計算すると

$$\begin{aligned}\iint_{D_R} \sqrt{R^2-x^2-y^2}dxdy &= \int_0^{2\pi} d\theta \int_0^R \sqrt{R^2-r^2}\,rdr \\ &= -\frac{2}{3}\pi\left[(R^2-r^2)^{\frac{3}{2}}\right]_0^R = \frac{2}{3}\pi R^3\end{aligned}$$

となる．一方南半球では $z=-\sqrt{R^2-x^2-y^2}$ であるが，外向きの法線ベクトルに伴う向きを xy 平面に正射影すると，通常の向きの逆になる．したがって，これらが相殺して第二項の積分は第一項の積分と同じ値になる．結局，求める面積分の値は

$$\int_{S_R} z\,dxdy = \frac{4}{3}\pi R^3$$

となる．

上記の面積分の値は，S_R が囲む半径 R の球体 V_R の体積と一致していることに注意してほしい．また，対称性から次の 2 つの面積分

$$\int_{S_R} x\,dydz, \quad \int_{S_R} y\,dzdx$$

も同じ値をもつことが分かる．

例題 9.5　図 9.4 のような，閉曲面 S に対して，S が囲む区域を D とする．このとき，等式

$$\iint_S z\,dxdy = \mathrm{Vol}\,D$$

が成立することを示せ．

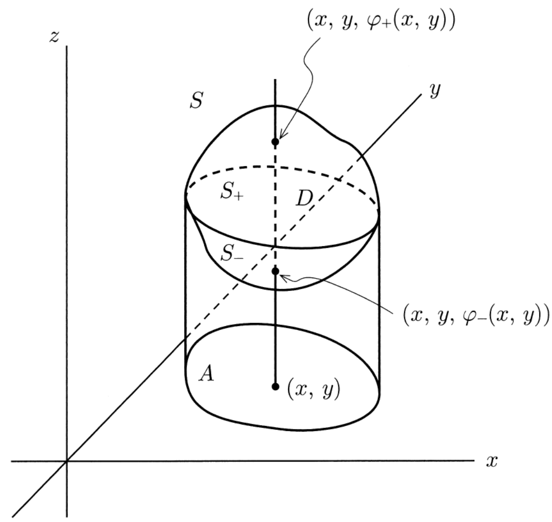


図 9.4　閉曲面.

解答　図 9.4 のように，任意の点 $(x, y) \in A$ で xy 平面に立てた垂線と曲面 S との交点の z 座標を，値が小さいほうからそれぞれ $\varphi_-(x,y), \varphi_+(x,y)$ とする．このとき S を下の部分 S_- と上の部分 S_+ の 2 つに分割すれば

$$\iint_S z\,dxdy = \iint_{S_+} z\,dxdy + \iint_{S_-} z\,dxdy$$

となるが，一方

$$\iint_{S_+} z\,dxdy = \iint_A \varphi_+(x,y)dxdy, \qquad \iint_{S_-} z\,dxdy = -\iint_A \varphi_-(x,y)dxdy$$

から

$$\iint_S z\,dxdy = \iint_A (\varphi_+(x,y) - \varphi_-(x,y))dxdy = \mathrm{Vol}\,D$$

となり，証明が終わる．

上記の証明は曲面 S が図 9.4 のような簡単な形をしているときにだけ通用するものである．しかし，実は例題 9.5 の主張は $\mathbb{R}^3$ 上の任意の閉曲面に対して成立する．さらに $z\,dxdy$ の替わりに $x\,dydz$ あるいは $y\,dzdx$ としても主張は成立する．S の形によっては，上記の議論を適宜修正することにより証明を与えることができる．読者はいろいろな形状の S に対して証明を工夫してみてほしい．

結局，図 9.5 のような閉曲面 S に対して，それが囲む区域を D とするとき

$$\mathrm{Vol}\,D = \frac{1}{3} \iint_S x\,dydz + y\,dzdx + z\,dxdy \tag{9.1}$$

という等式が得られることになる．この等式の幾何学的意味を述べると次のようになる．

S 上の点 $\mathrm{P} \in S$ の位置ベクトルを $\boldsymbol{r}$ とし，P を含む S の小区域を σ とす

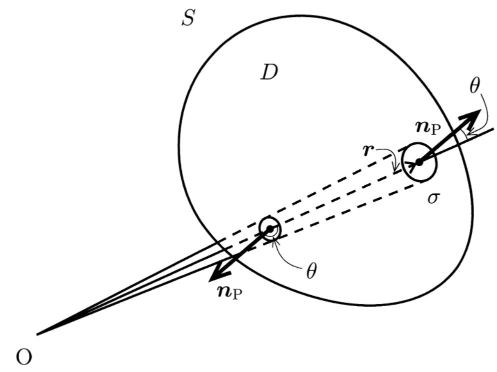


図 9.5　閉曲面の囲む体積.

る．このとき σ 上の各点と $\mathbb{R}^3$ の原点とを結んでできる円錐（図 9.5 参照）の体積は

$$\frac{1}{3} r \cos\theta \,\mathrm{Area}\,\sigma$$

により近似できる．ただし $|\boldsymbol{r}| = r$ で θ は $\boldsymbol{r}$ と法線ベクトル $\boldsymbol{n}_{\mathrm{P}}$ とのなす角度であり，$\theta > \pi$ の場合には負の値を取らせるものとする．こうすれば図 9.5 に示されているように符号付き体積はうまく相殺されて，S が囲む区域 D の体積だけが残って等式

$$\frac{1}{3}\int_S r\cos\theta\, d\sigma = \mathrm{Vol}\, D$$

が得られることになる．さてここで

$\boldsymbol{r}$ と x, y, z 軸の正の方向とのなす角度をそれぞれ λ, μ, ν

とすれば

$$\cos\theta = \cos\lambda\cos\alpha + \cos\mu\cos\beta + \cos\nu\cos\gamma$$

であり，また P の座標を (x, y, z) とすれば

$$r\cos\lambda = x, \quad r\cos\mu = y, \quad r\cos\nu = z$$

と書ける．これらを代入すれば

$$\frac{1}{3} r\cos\theta\, d\sigma = \frac{1}{3}(x\cos\alpha + y\cos\beta + z\cos\gamma)\, d\sigma = \frac{1}{3}(x\, dydz + y\, dzdx + z\, dxdy)$$

となり，式 (9.1) が確かに成立することが納得できるだろう．

（もりた・しげゆき，東京大学・東京工業大学名誉教授）

特　集（2014 年 6 月号予告）

数学と物理における空間概念

空間からみる数学と物理	河野　俊丈
特殊相対論と時空の幾何学	加藤　晃史
時空は曲がる	白水　徹也
量子力学とヒルベルト空間	加藤　光裕
古典力学からシンプレクティック幾何学へ	今野　宏
超弦理論と時空のコンパクト化	太田　信義
カラビ・ヤウ多様体と導来圏	戸田　幸伸
ミラー対称性	堀　健太朗

特　集（2014 年 4 月号）

物理現象における表現の多様さ

様々な視点がもたらす深い理解

巻頭言	和田　純夫
ニュートン力学と解析力学	加藤　光裕
ファラデーの力線とマクスウェル応力	岡部　洋一
量子力学の経路積分的見方	和田　純夫
多様な熱力学　エントロピーの 3 つの顔	佐々　真一
超伝導のマクロな見方とミクロな見方	加藤　雄介
一般相対性理論の幾何学的見方と非幾何学的見方　アインシュタインとの夢対話	米谷　民明
強結合と弱結合	今村　洋介
ホログラフィック原理の意味とその発展	江口　徹
《数学的な感覚の探求》　第 15 回	徳山　豪
《連載》　情報幾何の新展開　その 29	甘利　俊一
大学院入試問題からみた大学の数学　その 13	海老原　円 太田　雅人

編集後記

今回の特集はいかがでしたでしょうか．数理科学の代数的な構造が見て取れたかと思います．それと同時に代数の考え方も感じられたのではないでしょうか．特集で取り上げたテーマ以外にも代数的な構造が潜んでいる理論・現象はあるかと思います．皆様も探してみてはいかがでしょうか．

さて，今月号で 2 つの連載が最終回を迎えます．甘利先生の連載では情報幾何の面白さが，岡本先生の連載では科学の発展と社会の関わりは古くからあり，そこに様々な葛藤があったことが伝わったかと思います．次号以降では新しい連載が始まります．こちらも楽しみにしていただければ幸いです．　(R)

*　　*

代数学は，やや抽象的な印象があるのですが，その抽象性は言い換えれば汎用性の高さを意味しているとも思えます．そのように考えると，本特集で取り上げたように，代数学が様々な形で応用されていることにも頷けます．

ところで 3 月号の編集後記に書かせていただいたロマネスコという野菜について少し調べてみました．以前はブロッコリーのような野菜と書きましたが，正確にはカリフラワーの仲間とのことです．また，その構造がフィボナッチ数列と関連があるようで，これも一種の代数的構造なのかもしれません．読者の皆さんも興味があればぜひその構造を楽しんだ上で，召し上がってみて下さい．　(T)

数　理　科　学　5月号

2014 年 5 月 1 日発行

数 理 科 学 編 集 部　　発行人 木　下　敏　孝

TEL. (03) 5474–8816
FAX. (03) 5474–8817

ホームページ　http://www.saiensu.co.jp
ご意見・ご要望は　sk@saiensu.co.jp　まで．

発行所 ⓒ 株式会社 サ イ エ ン ス 社　TEL. (03) 5474–8500（代表）
〒 151–0051 東京都渋谷区千駄ヶ谷 1–3–25　振替 00170–7–2387　(03) 5474–8600 (広告部)

印刷・製本　三美印刷株式会社　山岡景仁